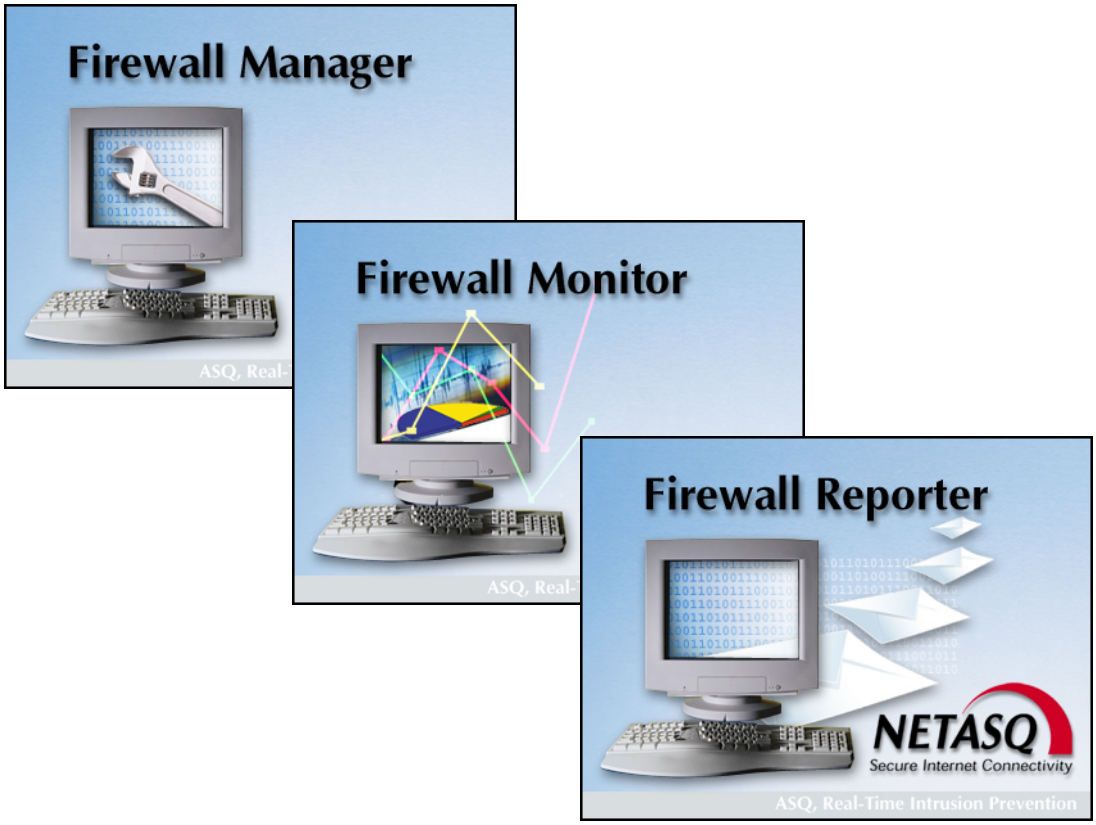
MANUEL D'UTILISATION - V6.3



MANUEL D'UTILISATION ET DE CONFIGURATION ADMINISTRATION SUITE V6.3.

- FIREWALL MANAGER
- FIREWALL REPORTER ET REPORTER PRO
- FIREWALL MONITOR
- FIREWALL SYSLOG

NETASQ
Secure Internet Connectivity

Référence : na_ug_ASv6.3_1206_fr
Date de création : Décembre 2006
Dernière modification : Décembre 2006

Sommaire

Sommaire 2
Avertissement 8
Hypothèses issues des critères communs 10

CHAPITRE I 12

GENERALITES 12

Introduction 13
Précautions d'utilisation 16
Dès la réception de votre IPS-Firewall 17
Présentation des boîtiers 18
Démontage du boîtier 24
Les capots 25

CHAPITRE II 26

INSTALLATION, PRE-CONFIGURATION, INTEGRATION 26

SECTION A 27
INTERFACE GRAPHIQUE 27
Introduction 28
Installation 29
Procédure de vérification 30
Enregistrement 32
SECTION B 33
L'IPS-FIREWALL NETASQ 33
Introduction 34
Préparation à l'installation physique du boitier 35
Mise en rack 37
Branchements 40
Pré-configuration 42
SECTION C 44
PREMIERE EXECUTION 44
Introduction 45
Démarrage de l'interface 46
Connexion à un IPS-Firewall 48
Fenêtre générale et menus 55
Fermer la session 57
SECTION D 58
INTEGRATION 58
Intégration 59

CHAPITRE III 60

CONFIGURATION RESEAU, OBJETS ET ASQ 60

SECTION A 61
CONFIGURATION RESEAU 61
Introduction 62
Présentation 63
Choix du mode d'utilisation 64
Configuration des interfaces 66
Configuration des VLANs 75
Configuration par DHCP 79
Configuration du dialup 81
Client DNS dynamique 85
Configuration du routage par interface 87
Routeur par défaut et routes statiques 89

© Copyright NETASQ 2006

Remarques 90
SECTION B 91
CONFIGURATION DES OBJETS 91
Introduction 92
Présentation 93
Utilisateurs 96
Machines 102
Réseaux 104
Plage d'adresses 105
Services 106
Protocoles 108
Groupe d'utilisateurs 109
Groupes 110
Groupe de services 111
Remarques 113
SECTION C 114
PREVENTION D'INTRUSION (ASQ) 114
Introduction 115
Présentation 116
Stateful 118
Translation 121
Routage 122
Analyse 123
Alarmes 124
Listes 129
Sonde 133
Plugins 134
CHAPITRE IV 137
NAT, FILTRAGE ET QOS 137
SECTION A 138
TRANSLATION D'ADRESSES 138
Introduction 139
Présentation 140
Edition d'un slot de translation 142
SECTION B 148
FILTRAGE 148
Introduction 149
Présentation 151
Remarques 153
Edition d'un slot de filtrage 154
Création des règles de filtrage 158
SECTION C 166
PROGRAMMATION HORAIRE 166
Programmateur de Slots 167
Calendriers 169
SECTION D 171
QOS : QUALITE DE SERVICE 171
Présentation 172
Configuration 173
Utilisation de la QoS 180
CHAPITRE V 183
VPN 183
Présentation 184
SECTION A 185
IPSEC 185
Introduction 186
Support de la fonctionnalité de NAT-T 194

© Copyright NETASQ 2006

Configuration 200
Règles de filtrage 213
Tunnels VPN passerelle à passerelle 215
SECTION B 223
PPTP 223
Introduction 224
Configuration 225
SECTION C 227
VPN SSL 227
Introduction 228
Configuration 229

CHAPITRE VI 237

CONFIGURATION DES PROXIES 237

SECTION A 238
PROXIES HTTP, SMTP ET POP3 238
Introduction 239
Redirection des flux vers les proxies 240
Proxy HTTP 241
Proxy SMTP 248
Proxy POP3 257
SECTION B 263
FILTRAGE DE CONTENU 263
Introduction 264
Antispam 265
Antivirus 272
Filtrage URL 277
Groupes d'URLs 279
Edition d'un slot filtrage URL 282
SECTION C 286
SERVICES 286
Agent SNMP 287
Serveur DHCP 291
Proxy DNS 295
Client NTP 298

CHAPITRE VII 300

CONFIGURATION DE L'AUTHENTIFICATION 300

Introduction 301
Configuration générale 302
Base LDAP 315
Introduction à la PKI 325
Configuration de la PKI 326
Procédure d'authentification 332
Enrôlement des utilisateurs 335
Sensibilisation des utilisateurs 339

CHAPITRE VIII 341

HAUTE DISPONIBILITE 341

Watchdog 342
Configuration 343
Haute disponibilité 344
Licences 345
Fonctionnement 346
Mise en place 348
Exemple d'architecture 352
Arrêt de la haute disponibilité 353
Remarques 354

© Copyright NETASQ 2006

CHAPITRE IX 355

GESTION DES TRACES 355

SECTION A 356
CONFIGURATION DES TRACES 356
Introduction 357
Paramétrage global 359
Mails 362
Evénements 363
Logs 364
SECTION B 366
RECEPTION DES ALARMES ET DES TRACES 366
Introduction 367
Présentation du Moniteur Temps réel 368
Remarques 369

CHAPITRE X 370

SAUVEGARDE ET MISE A JOUR 370

Introduction 371
Sauvegarde et restauration de la configuration 372
Sauvegarde et restauration du système 377
Mise à jour 378
Mise à jour WEB 381

CHAPITRE XI 384

ACTIONS DIVERSES 384

Introduction 385
Préférences 386
Règles implicites 391
Applications 393
Redémarrage de l'IPS-Firewall 394
Arrêt du firewall 395
Partition de démarrage 396
Licence 397
Modification des paramètres système 399
Sécurité 400
Configuration sécurisée 401
Quitter l'application 404
Active Update 405

CHAPITRE XII 407

NETASQ SYSLOG 407

Présentation 408
Remarques Importantes 409
SECTION A 410
INSTALLATION 410
Installation 411
Service Syslog 412
SECTION B 414
CONFIGURATION 414
Configuration du Firewall Manager 415
Configuration du NETASQ SYSLOG 416
SECTION C 418
EXPLOITATION DES LOGS 418
Exploitation des logs 419
Emplacement des logs 420

© Copyright NETASQ 2006

CHAPITRE XIII 421

MONITEUR TEMPS REEL 421

Introduction 422
SECTION A 423
FENETRE GENERALE 423
Les menus 424
Préférences 426
Carnet d'adresses 427
SECTION B 428
FENETRE DU MONITEUR 428
Ouverture d'un moniteur 429
Fenêtre principale 430
Global 432
Statistiques 435
ASQ 439
Tunnels IPSEC 444
Logs 446
Politique 449
SECTION C 451
OPTIONS 451
Actualisation des données 452
Comportement 453

CHAPITRE XIV 455

NETASQ REPORTER ET REPORTER PRO 455

Présentation 456
SECTION A 457
L'INTERFACE 457
Connexion 458
Fenêtre principale 461
Menus 465
SECTION B 467
UTILISATION 467
Connexion 468
Fichiers et Contenu 470
Gestionnaire de la base de données (Version PRO) 472
Colonnes et en-têtes 477
Constructeur de filtres (Version PRO) 481
Export des données 483
Graphiques 485
Statistiques 487
Services 489
Divers 492
Options 493
SECTION C 496
NETASQ LOG COLLECTOR (VERSION PRO) 496
Présentation 497
Service Log Collector 498
Configuration 499
Activité du Log Collector 505
SECTION D 506
NETASQ AUTOREPORT (VERSION PRO) 506
Introduction 507
Interface graphique 508
Mise en place du service 509
Construction des rapports 512

CHAPITRE XV 517

© Copyright NETASQ 2006

ANNEXES 517

Annexe A : Contrôle des saisies 518
Annexe B : Services TCP/IP 519
Annexe C : Codes ICMP 521
Annexe D : Exemples de translations d'adresses 522
Annexe E : Exemples de règles de filtrage 527
Annexe F : Evénements 538
Annexe G : Foire aux questions 539
Annexe H : Commandes 542
Annexe I : Rôle de la DMZ 545
Annexe J : Connexion au serveur SSH 546
Annexe K : Activation Key 547
Annexe L : Réinitialisation de l'IPS-Firewall 550
Annexe M : Noms interdits 552
Annexe N : Fichiers de traces NETASQ 553
Annexe O : Licences d'utilisation 560

© Copyright NETASQ 2006

Les informations contenues dans ce document sont susceptibles d'être modifiées sans préavis. Malgré tout le soin apporté à sa vérification, ce document peut comporter certaines erreurs. Dans ce cas, n'hésitez pas à prendre contact avec la société NETASQ.

La société NETASQ dégage par ailleurs toute responsabilité quant aux erreurs qui peuvent exister dans ce document et aux dommages qui pourraient en résulter.

Acceptation des termes de la licence

En ouvrant l'emballage du Produit ou en installant le logiciel d'administration, vous acceptez et serez lié aux termes et restrictions de cette licence.

Licence

NETASQ, par la présente licence et si vous en acceptez les termes, concède le droit d'usage non exclusif et non transférable du code programme du Produit. Vous n'avez pas l'autorisation de copier tout ou partie du programme ou de la notice associés au Produit. Vous acceptez que le code source du Produit, le concept et les idées liées au Produit restent valablement la propriété intellectuelle de NETASQ. Vous acceptez de ne pas copier, désassembler, décompiler, ou dériver tout ou partie du Produit, ou de développer un autre produit reprenant le concept ou les idées contenus dans ce Produit. Toute violation de cette obligation engagerait votre responsabilité et vous rendrait redevable de dommages-intérêts au bénéfice de NETASQ.

Limites de garanties et de responsabilités

1. Matériel

NETASQ garantit les produits matériels des défauts de pièces et main d'œuvre pour une période d'un an, sauf indication contraire au tarif valide à la date de commande du client. Cette période commence à la date d'envoi si le matériel est installé par le client, à la date d'installation si celle-ci est effectuée par NETASQ.

2. Logiciel

Les produits logiciels NETASQ, ci-après désignés « les Logiciels », sont garantis pour une période de 90 jours (sauf mention particulière précisée à l'achat) à compter de la date d'activation du produit contre les défauts et les dysfonctionnements substantiels par rapport au manuel tel qu'il existe à la date de livraison et sous les environnements et leur version supportés par le Produit.

NETASQ ne garantit pas le Logiciel ou le Produit pour des usages sous d'autres environnements logiciels et réseaux que ceux préconisés spécifiquement.

3.

En cas de défaut, la responsabilité de NETASQ et le seul recours du client consistent, sur décision de NETASQ, soit au remboursement des sommes reçues au titre de la vente du Produit annulant ainsi la présente Licence d'utilisation, soit à la réparation ou le remplacement du Produit ou support.

4.

A l'exception de la garantie limitée telle que décrite dans les paragraphes précédents, ce produit est fourni " tel quel " sans autre garantie de quelque sorte, implicite ou explicite. NETASQ ne garantit pas que le Produit correspondra à votre besoin ou que son utilisation pourra être ininterrompue et exempte d'erreurs. NETASQ rejette toute garantie ou obligation commerciale considérée par le client comme implicite, ne peut garantir que le produit convient à tous les cas particuliers ni ne prend de responsabilités en cas d'usage frauduleux ou illégal.

© Copyright NETASQ 2006

5.

En aucun cas NETASQ ne pourra être tenue pour responsable des dommages subis par vous ou tout autre tiers, en dehors de ceux explicitement mentionnés dans cet agrément, qu'ils soient directement ou indirectement liés à l'usage du Produit, y compris d'éventuelles pertes d'exploitations dues à une interruption de service ou tout autre cause, même si NETASQ a été avisée de la possibilité de tels dommages. La responsabilité maximale de NETASQ en cas de dommages se limite au montant reçu par NETASQ pour l'achat du Produit en particulier qui a pu causer ces dommages.

Tout litige éventuel relatif à la défectuosité alléguée du logiciel considéré devra être obligatoirement soumis à la compétence des juridictions du siège de NETASQ, le droit français étant seul applicable.

Attention, certains Produits de NETASQ permettent de récupérer et d'analyser des traces. Ces informations permettent un contrôle de l'activité des utilisateurs internes et peuvent fournir des informations nominatives. La législation en vigueur, dans le pays destinataire, peut imposer d'appliquer certaines mesures (telles que notamment des déclarations administratives ou autres) lorsque des personnes sont soumises à un tel contrôle. Assurez-vous que ces éventuelles mesures ont bien été mises en application avant toute utilisation du produit.

Certains Produits de NETASQ fournissent des mécanismes de chiffrement de données dont l'usage peut être interdit ou limité par la législation en vigueur dans le pays destinataire. Malgré le contrôle réalisé par NETASQ à l'exportation, assurez vous que vous êtes dans la légalité pour utiliser pleinement ou partiellement les produits NETASQ.

NETASQ dégage toute responsabilité quant à l'utilisation du présent produit dans un cadre sortant de la légalité pour le pays de destination.

L'installation d'un IPS-Firewall s'inscrit bien souvent dans la mise en place d'une politique de sécurité globale. Pour garantir une protection optimale de vos biens, ressources ou informations, il ne s'agit pas seulement d'installer l'IPS-Firewall entre votre réseau et l'Internet. Notamment parce que la plupart des attaques viennent de l'intérieur (accident, personne mécontente de son travail, personne licenciée ayant gardé un accès interne…). Mais aussi parce que l'on conviendra qu'il ne sert à rien d'installer une porte blindée si les murs sont en papier.

Sous l'impulsion des critères communs, NETASQ vous propose donc de prendre en compte les hypothèses d'utilisation de la suite d'administration et du produit IPS-Firewall énoncées ci-dessous. Ces hypothèses vous exposent les exigences d'utilisation à respecter pour garantir le fonctionnement de votre IPS-Firewall dans le cadre de la certification aux critères communs.

Hypothèses sur les mesures de sécurité physiques

Les boîtiers appliances IPS-Firewall/VPN sont installés et stockés conformément à l'état de l'art concernant les dispositifs de sécurité sensibles : local à accès protégé, câbles blindés en paire torsadée, étiquetage des câbles, etc.

Hypothèses sur les mesures de sécurité organisationnelles

Un rôle administrateur particulier, le super-administrateur, présente les caractéristiques suivantes :

► Il est le seul à être habilité à se connecter via la console locale sur les boîtiers appliances IPS-Firewall/VPN, et ce uniquement lors de l'installation de l'IPS-Firewall ou pour des opérations de maintenance, en dehors de l'exploitation,

► Il est chargé de la définition des profils des autres administrateurs,

► Tous les accès dans les locaux où sont stockés les boîtiers appliances IPS-Firewall/VPN se font sous sa surveillance, que l'accès soit motivé par des interventions sur l'appliance ou sur d'autres équipements. Toutes les interventions sur les boîtiers appliances IPS-Firewall/VPN se font sous sa responsabilité.

Les mots de passe des utilisateurs et des administrateurs doivent être choisis de façon à retarder toutes les attaques visant à les casser, via une politique de création et/ou de contrôle de ceux-ci (par ex : mélange alphanumérique, longueur minimum, ajout de caractères spéciaux, pas de mots des dictionnaires usuels, etc.).

Il est de la responsabilité des administrateurs de sensibiliser tous les utilisateurs à ces bonnes pratiques (voir Chapitre VI, configuration de l'authentification, sensibilisation des utilisateurs).

La politique de contrôle des flux d'informations à mettre en œuvre est définie, pour tous les équipements des réseaux dits « Trusted » à protéger, de manière :

► complète : les cas d'utilisation standards des équipements ont tous été envisagés lors de la définition des règles et leurs limites autorisées ont été définies,

► stricte : seuls les cas d'utilisation nécessaires des équipements sont autorisés,

► correcte : les règles ne présentent pas de contradiction,

► non-ambiguë : l'énoncé des règles fournit tous les éléments pertinents pour un paramétrage direct de l'appliance par un administrateur compétent.

© Copyright NETASQ 2006

Hypothèses relatives aux agents humains

Les administrateurs sont des personnes non hostiles et compétentes, disposant des moyens nécessaires à l'accomplissement de leurs tâches. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité. Notamment, leur compétence et leur organisation implique que :

► Différents administrateurs avec les mêmes droits ne mènent des actions d'administration qui se contredisent (ex : modifications incohérentes de politique de contrôle des flux d'information).

► L'exploitation des journaux et le traitement des alarmes sont effectués dans les délais appropriés.

Hypothèses sur l'environnement de sécurité TI

Les boîtiers appliances IPS-Firewall/VPN sont installés conformément à la politique d'interconnexion des réseaux en vigueur et sont les seuls points de passage entre les différents réseaux sur lesquels il faut appliquer la politique de contrôle des flux d'information. Les périphériques de connexion (modem) sont interdits sur les réseaux dits « Trusted ».

A part l'application des fonctions de sécurité, les boîtiers appliances IPS-Firewall/VPN ne fournissent pas de service réseau autre que le routage et la translation d'adresse (ex : pas de DHCP, DNS, PKI, proxies applicatifs, etc.). Les boîtiers appliances IPS-Firewall/VPN ne sont pas configurés pour retransmettre les flux IPX, Netbios, Appletalk, PPPoE ou IPv6. Rappel : ces services sont disponibles sur un IPS-Firewall mais ne font pas partie du cadre d'évaluation des critères communs.

L'IPS-Firewall ne dépend pas de services externes (DNS, DHCP, RADIUS, etc.) pour l'application de la politique de contrôle des flux d'information. Rappel : ces services sont disponibles sur un IPS-Firewall mais ne font pas partie du cadre d'évaluation des critères communs.

Les stations d'administration à distance sont sécurisées et maintenues à jour de toutes les vulnérabilités connues concernant les systèmes d'exploitation et les applications hébergées. Elles sont exclusivement dédiées à l'administration des IPS-Firewalls.

Les équipements réseau avec lesquels la TOE établit des tunnels VPN sont soumis à des contraintes de contrôle d 'accès physique,de protection et de maîtrise de leur configuration équivalentes à celles des boîtiers appliances firewall-VPN de la TOE.

Les postes sur lesquels s 'exécutent les clients VPN des utilisateurs autorisés sont soumis à des contraintes de contrôle d' accès physique, de protection et de maîtrise de leur configuration équivalentes à celles des postes clients des réseau de confiance. Ils sont sécurisés et maintenus à jour de toutes les vulnérabilités connues concernant les systèmes d 'exploitation et les applications hébergées.

Que sont les Critères Communs ?

Les critères communs évaluent (sur une échelle « EAL » de 1 à 7) les capacités d'un produit à fournir les fonctions de sécurité pour lesquelles il a été conçu, ainsi que la qualité de son cycle de vie (développement, production, livraison, mise en service, mise à jour). Ils sont une convergence des différentes normes de qualité (en matière de sécurité) imaginées depuis 1980 :

► Orange Book – DoD,
► CTCPEC (Canadian Trusted Computer Product Evaluation Criteria),
► ITSEC (Information Technology Security Evaluation Criteria),
► TCSEC (Trusted Computer System Evaluation Criteria).

© Copyright NETASQ 2006

Chapitre I

Généralités

© Copyright NETASQ 2006

Principe

Destinés à sécuriser des structures de toutes tailles, les IPS-Firewalls de la gamme NETASQ sont des boîtiers pré-configurés : pas d'installation matérielle, ni d'installation logicielle, pas de compétences Unix nécessaires mais une configuration conviviale au moyen d'une interface graphique.

L'IPS-Firewall NETASQ permet de définir les règles de contrôle d'accès entrant ou sortant. Son concept est simple : toute transmission entrante ou sortante transitant par le Firewall NETASQ est contrôlée, autorisée ou refusée suivant les règles, paquet par paquet.

L'IPS-Firewall NETASQ est basé sur un mécanisme de filtrage de paquets évolué qui procure un haut niveau de sécurité. Tous les IPS-firewalls NETASQ intègrent la technologie ASQ (Active Security Qualification), développée par NETASQ. Cette technologie permet la détection et le blocage, en temps réel, d'attaques informatiques : paquets illégaux, tentatives de déni de service, anomalies dans une connexion, scans de ports, buffer overflow...

En cas de tentative d'intrusion, selon les consignes spécifiées dans la politique de sécurité, le Firewall NETASQ bloque la transmission, génère une alarme et mémorise les informations liées au paquet ayant provoqué l'alarme. Ainsi, il vous est possible d'analyser l'attaque et de rechercher son origine.

L'IPS-Firewall permet non seulement d'empêcher, ou de limiter à certains services, les connexions entrantes sur votre réseau mais aussi de contrôler l'utilisation de l'Internet faite par vos utilisateurs internes (HTTP, FTP, SMTP ...). Le contrôle des utilisateurs peut aussi être réalisé au moyen d'une authentification via une base d'authentification interne ou externe.

L'IPS-Firewall NETASQ gère également les mécanismes de translations d'adresses et de ports. Ces mécanismes apportent sécurité (en masquant votre adressage interne), flexibilité (en permettant d'utiliser un plan d'adressage interne privé quelconque) et réduction de coût (en permettant la mise à disposition de plusieurs serveurs sur Internet avec une seule adresse IP publique).

Avec la nouvelle version de l'ASQ, le moteur IPS (Intrusion Prevention System) de NETASQ, un IPS-firewall NETASQ offre d'autant plus de sécurité. Son architecture à plug-in permet de contrôler la majeure partie du trafic circulant au travers du firewall même au niveau applicatif. Ses performances en matière de débit, de nombres de règles, de tunnels, sont décuplées.

Grâce à son interface utilisateur sous Windows, il offre la possibilité de définir rapidement et simplement les règles de sécurité pour votre réseau, à partir d'un poste local sous Windows. Vous pouvez aussi monitorer, en temps réel, l'activité de votre firewall.

L'IPS-Firewall NETASQ est également doté de fonctions avancées de traçabilité. En cas de tentative d'intrusion, l'administrateur du réseau peut accéder à l'ensemble des données envoyées avant l'attaque et voir comment elle est préparée. Le NETASQ REPORTER vous apportera une vision graphique et une analyse fine des logs générés sur le firewall.

Enfin, l'IPS-Firewall NETASQ intègre les fonctionnalités de passerelle VPN vous permettant d'établir des tunnels chiffrés avec d'autres équipements VPN. Ainsi, vos communications inter-sites ou avec vos utilisateurs nomades ("Road Warriors") peuvent être sécurisées même en utilisant une infrastructure de communication non sûre comme l'est Internet.

© Copyright NETASQ 2006

A qui s'adresse cette notice

Cette notice s'adresse à un administrateur réseau ou tout au moins à un utilisateur possédant un minimum de connaissances sur IP.

Pour configurer efficacement votre IPS-Firewall NETASQ, vous devez connaître le fonctionnement d'IP, de ses protocoles et de leurs particularités :

- ICMP (Internet Control Message Protocol),
- IP (Internet Protocol),
- TCP (Transmission Control Protocol),
- UDP (User Datagram Protocol).

La connaissance du fonctionnement général des principaux services TCP/IP est appréciable :

- HTTP,
- FTP,
- Messagerie (SMTP, POP3, IMAP),
- telnet,
- DNS,
- DHCP,
- .SNMP,
- NTP.

Si vous ne possédez pas ces connaissances, ne vous inquiétez pas : l'acquisition d'un ouvrage généraliste sur TCP/IP vous les apportera.

Meilleure est votre connaissance de TCP/IP, meilleures seront vos règles de filtrages et meilleure sera votre sécurité IP.

A la réception de votre IPS-Firewall NETASQ

A la réception de votre IPS-Firewall NETASQ, veuillez vérifier les points suivants avant d'effectuer toute opération sur votre produit :

- le packaging intérieur et extérieur n'est pas endommagé et les bandes de garantie n'ont pas été rompues,
- l'étiquette de garantie apposée sur le boîtier n'est pas rompue,

Si les bandes de garantie ou les étiquettes de garantie sont rompues, contactez immédiatement votre partenaire,

Conservez précieusement le carton d'emballage, dans l'éventualité d'un transport. Il a été conçu pour assurer une protection optimale de votre Firewall NETASQ (résistance aux chocs, aux températures...).

A la livraison, vérifiez que dans l'emballage se trouvent bien :

- l'IPS-Firewall NETASQ,
- un cordon secteur,
- un câble série croisé DB9F (sauf modèles F50),
- un câble croisé RJ 45,
- le CD-ROM du logiciel de configuration à distance pour Windows,
- une feuille contenant le mot de passe Web.

Si un élément est manquant, n'hésitez pas à contacter votre revendeur.

© Copyright NETASQ 2006

Administration Suite et Administration Suite PRO

NETASQ propose deux outils de configuration des firewalls, la suite d'administration Standard et la suite d'administration PRO. La principale différence qui réside entre ces deux suites et l'intégration du REPORTER PRO dans la suite d'administration PRO.

Contenu des packages

Admininstration Suite STANDARD

Menu CLIENT

- ► Manager,
- ► Moniteur,
- ► Reporter.

Menu SERVEUR

- ► Syslog.

Admininistration Suite PRO

Menu CLIENT

- ► Manager,
- ► Moniteur,
- ► Reporter PRO.

Menu SERVEUR

- ► Syslog,
- ► Collector,
- ► MYSQL,
- ► Autoreport.

Le menu CLIENT constitue l'ensemble des outils de configuration graphique des suites NETASQ servant d'interface entre l'utilisateur et l'appliance. Ces outils sont installés sur une station d'administration.

Le menu SERVEUR constitue quant à lui l'ensemble des outils de communication utilisé pour récupérer les logs auprès des appliances vous appartenant. Ces outils sont généralement installés sur une machine dédiée du fait des ressources qu'elles nécessitent.

L'utilisation de piles LITHIUM de mauvais type peut entraîner l'explosion des composants. Veuillez suivre les spécifications du constructeur de piles LITHIUM (utilisées dans votre IPS-Firewall) pour le recyclage des piles usagées.

L'IPS-Firewall doit être installé conformément à l'état de l'art correspondant aux modalités pratiques d'installation sécurisée à savoir : dans un local ou bureau à accès protégé. Pour garantir l'intégrité de l'appliance et la non compromission de la sécurité de votre installation, tous les accès (à l'IPS-Firewall) non autorisés doivent être évités.

Veillez à placer les équipements lourds dans la partie basse de l'armoire ou du rack et les éléments plus légers dans la partie haute.

Assurez vous que l'alimentation est correctement raccordée à la terre, correspondant aux spécifications NETASQ concernant l'alimentation des IPS-Firewalls. De plus il est préférable de protéger l'alimentation par des équipements de type UPS.

Dans le cas des F25 et F50, notez que débrancher le câble d'alimentation de l'embase secteur permet de déconnecter l'appliance du secteur. Un bouton ON/OFF est disponible sur les autres produits.

Veillez à débranchez TOUS les câbles d'alimentation (les deux câbles sur le F1000 et les trois câbles sur les F2000/25000) reliés au boîtier avant toute intervention sur l'appliance.

L'installation de l'IPS-Firewall NETASQ doit être réalisée dans un environnement où la température n'excède pas 35°C.

Assurez-vous que rien n'obstrue les ouies de ventilation du produit afin de garantir une circulation de l'air optimale.

Les poignées métalliques présentes sur la face avant des produits F1000, F2000 et F5000 ne doivent pas être utilisées pour porter celui-ci mais uniquement pour placer ou sortir l'appliance dans la baie.

© Copyright NETASQ 2006

Intégrité de votre produit

Afin de garantir l'intégrité de votre produit, NETASQ a mis en place plusieurs mécanismes. Vérifiez ces mécanismes pour valider que votre produit n'a pas été manipulé frauduleusement :

► **Les étiquettes** : chaque IPS-Firewall est livré avec un carton sur lequel est apposé deux étiquettes contenant des informations d'identification du produit contenu et de sa version. De plus une étiquette « Numéro de série » est apposée directement sur le produit. Vérifiez que ces informations concordent avec votre commande.

► **La scellée du carton** : chaque IPS-Firewall est livré avec un carton sur lequel est apposé une bande de garantie spécifique à NETASQ. Vérifier la présence de cette bande de garantie sur le carton de votre produit :

NETASQ
Firewall & VPN Solutions
BANDE DE GARANTIE
ATTENTION ! Si cette bande est détériorée, prière de FAIRE LES RESERVES D'USAGE AUPRES DU TRANSPORTEUR A RECEPTION DES COLIS.
NETASQ
3, rue Archimède
59650 VILLENEUVE D'ASCQ
FRANCE
Tel: +33 320 619 630 Fax : +33 320 619 639
GUARANTEE TAPE
WARNING ! If this tape has been tampered with, please EXPRESS YOUR RESERVATION TO THE CARRIER UPON RECEIPT OF THE PARCELS.

Si cette bande est absente, contactez votre revendeur au plus vite pour connaître les raisons de l'ouverture du carton.

► **La scellée de l'IPS-Firewall** : une étiquette de scellée est apposée sur tous les IPS-Firewalls. Il est alors impossible de remplacer ou de modifier un des éléments hardware de la solution. Cette étiquette a la particularité d'afficher un message (VOID) qui ne peut plus être effacé lorsqu'elle est décollée. Il existe deux types de scellée : une apposée par NETASQ en sortie de production et une apposée par votre partenaire si une opération de maintenance doit être réalisée sur votre produit (cette opération de maintenance doit vous être expliquée par votre partenaire par l'intermédiaire d'un certificat d'activité).

Valider ces mécanismes de sécurité vous assure de l'intégrité du produit reçu. N'hésitez pas à contacter votre revendeur si un de ces éléments n'était pas conforme à leur description.

Contenu du packaging

Conservez précieusement le carton d'emballage, dans l'éventualité d'un transport. Il a été conçu pour assurer une protection optimale de votre IPS-Firewall NETASQ (résistance aux chocs, aux températures élevées...). A la livraison, vérifiez que dans l'emballage se trouvent bien :

► L'IPS-Firewall NETASQ du modèle commandé,
► Un cordon secteur (réf. 1076036),
► Un câble série croisé DB9F (réf. 1076033),
► Un câble croisé RJ 45 (câble bleu, réf. 1076034),
► Le CD-ROM de la suite logicielle NETASQ (Administration Suite),
► Les équerres et système de fixation pour mise en rack 19 pouces *,
► Les conditions générales de services.

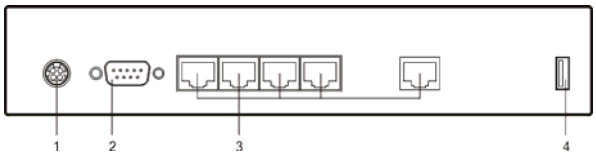
Si un élément est manquant, n'hésitez pas à contacter votre revendeur.

*selon modèle et sur demande pour les F50.

© Copyright NETASQ 2006

F25

Face Arrière



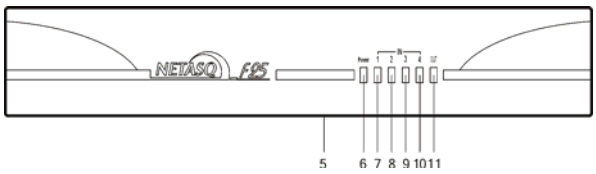
1. Embase Secteur : le branchement du cordon d'alimentation.
2. Port série : pour la connexion directe de l'IPS-Firewall avec un PC ou un modem.
3. Ports Ethernet 10/100Mbits/s de type RJ45 : pour le branchement des câbles réseau

   ► Interface identifiée 1-4 : Interne
   ► Interface identifiée 5 : Externe

Ces interfaces sont de type SELV (Safety Extra Low Voltage).

4. Port USB.

Face Avant



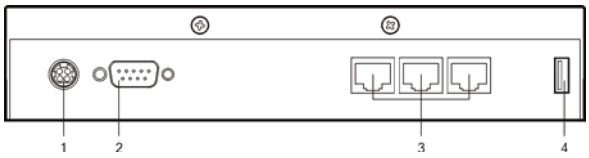
5. Bouton Reset : pressez 10 secondes pour restaurer la configuration par défaut.
6. Voyant Power : l'IPS-Firewall est sous tension lorsque la LED est allumée.
7-11. Voyant Interface 1-5

Si la LED d'un voyant d'interface est éteinte, l'interface correspondante n'est pas active, aucun câble réseau n'est connecté à cette interface ou aucun trafic ne passe par l'interface.

Si la LED d'un voyant clignote, l'interface fonctionne correctement, le trafic passe dans l'interface.

F50

Face Arrière



1. Embase Secteur : le branchement du cordon d'alimentation.
2. Port série : pour la connexion directe de l'IPS-Firewall avec un PC ou un modem.
3. Ports Ethernet 10/100Mbits/s de type RJ45 : pour le branchement des câbles réseau

© Copyright NETASQ 2006

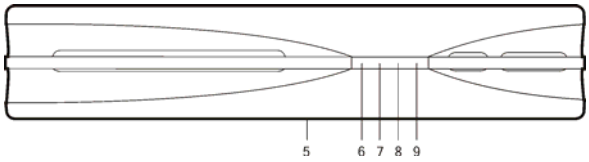
► Interface identifiée 1 : Interne
► Interface identifiée 2 : Externe
► Interface identifiée 3 : DMZ

Ces interfaces sont de type SELV (Safety Extra Low Voltage).

ATTENTION : l'ordre des ports de la nouvelle génération des F50 NETASQ (en production depuis novembre 2004) est différent de celui des F50 ancienne génération. Reportez vous à la Note technique « Inversion des ports sur le F50 » disponible sur le site WEB NETASQ pour plus d'informations.

4. Port USB.

Face Avant



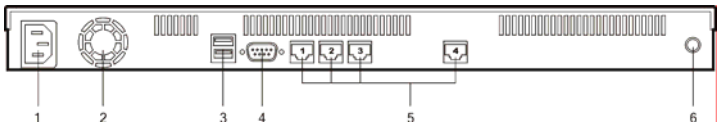
5. Bouton Reset : pressez 10 secondes pour restaurer la configuration par défaut.
6. Voyant Power : l'IPS-Firewall est sous tension lorsque la LED est allumée.
7. Voyant Interface 1
8. Voyant Interface 2
9. Voyant Interface 3

Si la LED d'un voyant d'interface est éteinte, l'interface correspondante n'est pas active, aucun câble réseau n'est connecté à cette interface ou aucun trafic ne passe par l'interface.

Si la LED d'un voyant clignote, l'interface fonctionne correctement, le trafic passe dans l'interface.

F200

Face Arrière



1. Embase Secteur : le branchement du cordon d'alimentation.
2. Grille Ventilateur.
3. Port USB
4. Port série : pour la connexion directe de l'IPS-Firewall avec un PC ou un modem.
5. Ports Ethernet 10/100Mbits/s de type RJ45 : pour le branchement des câbles réseau

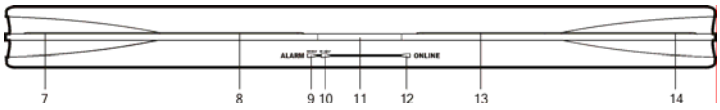
► Interface identifiée 1 : Externe
► Interface identifiée 2 : Interne
► Interface identifiée 3 : DMZ

Ces interfaces sont de type SELV (Safety Extra Low Voltage).

Attention, si le produit a été commandé dans une version 2 ports, les interfaces 3 et 4 ne sont pas actives. S'il a été commandé dans une version 3 ports, l'interface 4 n'est pas active.

6. Bouton On/Off : bouton d'arrêt et de mise en marche de l'appliance.

Face Avant



7. Voyant Interface 4
8. Voyant Interface 3
9. Alarmes mineures : une alarme mineure a été détectée si la LED clignote (200ms).
10. Alarmes majeures : une alarme majeure a été détectée si la LED est allumée.
11. Voyant Power : l'IPS-Firewall est sous tension lorsque la LED est allumée.
12. Voyant Online
13. Voyant Interface 2
14. Voyant Interface 1

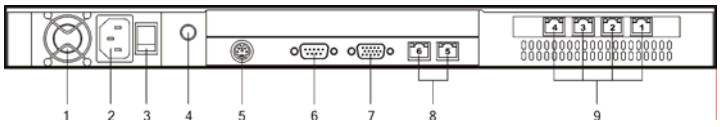
Le voyant Online clignote lors du démarrage de l'appliance, se fixe une fois que le système est opérationnel et s'éteint (dans le cas de la HA) pour signifier qu'il est en mode passif.

Si la LED d'un voyant d'interface est éteinte, l'interface correspondante n'est pas active, aucun câble réseau n'est connecté à cette interface ou aucun trafic ne passe par l'interface.

Si la LED d'un voyant clignote, l'interface fonctionne correctement, le trafic passe dans l'interface.

F500

Face Arrière



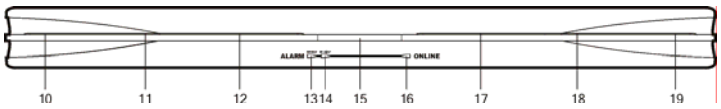
1. Grille Ventilateur.
2. Embase Secteur : le branchement du cordon d'alimentation.
3. Bouton d'arrêt et de mise en marche de l'alimentation de l'appliance.
4. Bouton On/Off : bouton d'arrêt et de mise en marche de l'appliance.
5. Port mini-din : pour le branchement d'un clavier.
6. Port série : pour la connexion directe de l'IPS-Firewall avec un PC ou un modem.
7. Port VGA : pour le branchement d'un écran.
8. Ports Gigabits de type RJ45 : pour le branchement des câble réseau (interface DMZ).
9. Ports Ethernet 10/100Mbits/s de type RJ45 : pour le branchement des câbles réseau

   ► Interface identifiée 1 : Externe
   ► Interface identifiée 2 : Interne
   ► Interface identifiée 3 : DMZ

Ces interfaces sont de type SELV (Safety Extra Low Voltage).

Attention, si le produit est commandé avec moins d'interface que le maximum prévu (6, dont 2 gigabits) les interfaces non souscrites ne sont pas actives.

Face Avant

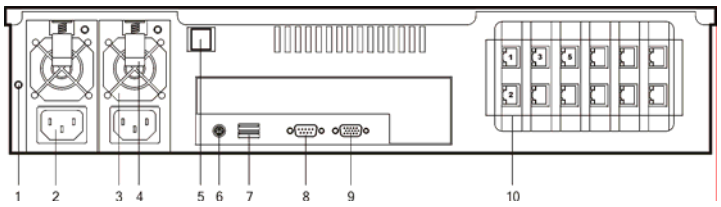


10. Voyant Interface 5 : interface Gigabit (LED orange).
11. Voyant Interface 1
12. Voyant Interface 2
13. Alarmes mineures : une alarme mineure a été détectée si la LED clignote (200ms).
14. Alarmes majeures : une alarme majeure a été détectée si la LED est allumée.
15. Voyant Power : l'IPS-Firewall est sous tension lorsque la LED est allumée.
16. Voyant Online
17. Voyant Interface 3
18. Voyant Interface 4
19. Voyant Interface 6 : interface Gigabit (LED orange).

Veuillez vous reportez à la section F200 pour plus d'informations sur le fontionnement des voyants.

F1000

Face Arrière



1. Bouton d'arrêt de l'alarme.
2. Deux embases secteur : pour le branchement de deux cordons d'alimentation. Le F1000 est équipé d'une alimentation redondante. Chaque bloc secteur de l'alimentation doit être relié à un secteur électrique différent.
3. Grille Ventilateur.
4. Démontage de l'alimentation.
5. Bouton On/Off : bouton d'arrêt et de mise en marche de l'appliance.
6. Port mini-din : pour le branchement d'un clavier.
7. Port USB
8. Port série : pour la connexion directe de l'IPS-Firewall avec un PC ou un modem.
9. Port VGA : pour le branchement d'un écran.
10. 4 à 12 ports Ethernet de type RJ45, pour le branchement des câbles réseau. Les cartes d'extension de ports Ethernet peuvent être achetées séparément. Des ports Gigabits sont aussi disponibles sur le F1000.

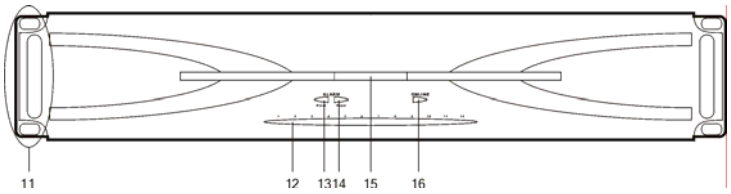
- ► Interface identifiée 1 : Externe
- ► Interface identifiée 2 : Interne
- ► Interface identifiée 3 : DMZ

Ces interfaces sont de type SELV (Safety Extra Low Voltage).

Lorsqu'un des blocs d'alimentation n'est plus opérationnel, une alarme sonore se déclenche et peut être arrêtée grâce au bouton d'arrêt de l'alarme. Attention, si vous ne branchez qu'un seul câble d'alimentation, l'alarme se mettra en route également. Une fois l'alarme coupée vous ne pourrez plus être averti d'un problème sur l'alimentation.

© Copyright NETASQ 2006

Face Avant



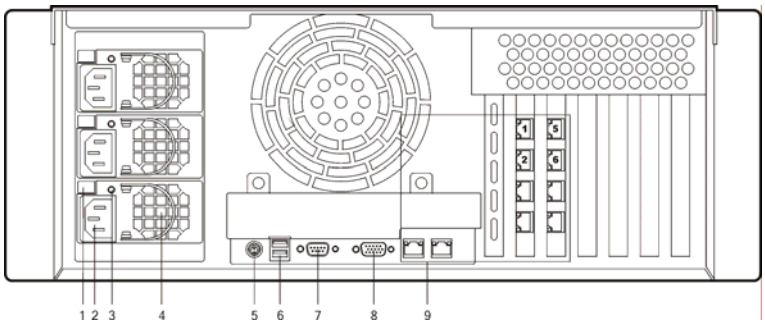
11. Poignées et oreilles métalliques sur châssis.
12. Voyants Interfaces.
13. Alarmes mineures : une alarme mineure a été détectée si la LED clignote (200ms).
14. Alarmes majeures : une alarme majeure a été détectée si la LED est allumée.
15. Voyant Power : l'IPS-Firewall est sous tension lorsque la LED est allumée.
16. Voyant Online

Le voyant Online clignote lors du démarrage de l'appliance, se fixe une fois que le système est opérationnel et s'éteint (dans le cas de la HA) pour signifier qu'il est en mode passif.

Si la LED d'un voyant d'interface est éteinte, l'interface correspondante n'est pas active, aucun câble réseau n'est connecté à cette interface ou aucun trafic ne passe par l'interface. Si la LED d'un voyant clignote, l'interface fonctionne correctement, le trafic passe dans l'interface.

F2000/F5000

Face Arrière



1. Démontage de l'alimentation.
2. Trois embases secteur : pour le branchement de trois cordons d'alimentation. Le F5000 est équipé d'une alimentation redondante. Chaque bloc secteur de l'alimentation doit être relié à un secteur électrique différent.
3. Bouton d'arrêt de l'alarme.
4. Grille Ventilateur.
5. Port mini-din : pour le branchement d'un clavier.
6. Port USB
7. Port série : pour la connexion directe de l'IPS-Firewall avec un PC ou un modem.
8. Port VGA : pour le branchement d'un écran.
9. 4 à 24 ports Ethernet de type RJ45 (4 à 20 ports pour le F2000 dont 4 Giga et 4 à 24 ports Giga pour le F5000), pour le branchement des câbles réseau. Les cartes d'extension de ports Ethernet peuvent être achetées séparément. Des ports Gigabits sont aussi disponibles sur le F5000.

- ► Interface identifiée 1 : Externe
- ► Interface identifiée 2 : Interne
- ► Interface identifiée 3 : DMZ

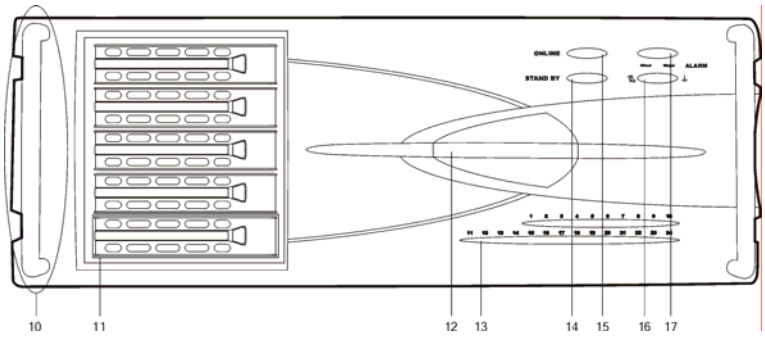
Les caractéristiques électriques de l'appareil sont les suivantes : 100-240V 50/60Hz 6A.

© Copyright NETASQ 2006

Ces interfaces sont de type SELV (Safety Extra Low Voltage).

Lorsqu'un des blocs d'alimentation n'est plus opérationnel, une alarme sonore se déclenche et peut être arrêtée grâce au bouton d'arrêt de l'alarme. Attention, si vous ne branchez qu'un seul câble d'alimentation, l'alarme se mettra en route également. Une fois l'alarme coupée vous ne pourrez plus être averti d'un problème sur l'alimentation.

Face Avant



10. Poignées et oreilles métalliques sur châssis.
11. Disque RAID et leur système de démontage.
12. Voyant Power : l'IPS-Firewall est sous tension lorsque la LED est allumée.
13. Voyants Interfaces.
14. Bouton « Stand By » : bouton d'arrêt et de mise en marche de l'appliance.
15. Voyant Online
16. Voyants de défaillance : alimentation à gauche et surchauffe à droite.
17. Alarmes mineures et majeures : une alarme mineure a été détectée si la LED de gauche clignote (200ms) et une alarme majeure a été détectée si la LED de droite est allumée.

Le voyant Online clignote lors du démarrage de l'appliance, se fixe une fois que le système est opérationnel et s'éteint (dans le cas de la HA) pour signifier qu'il est en mode passif.

Si la LED d'un voyant d'interface est éteinte, l'interface correspondante n'est pas active, aucun câble réseau n'est connecté à cette interface ou aucun trafic ne passe par l'interface.

Si la LED d'un voyant clignote, l'interface fonctionne correctement, le trafic passe dans l'interface.

© Copyright NETASQ 2006

Démontage du boîtier

En aucun cas vous ne pouvez démonter le boîtier du Firewall NETASQ.

Seule la société NETASQ et ses agents de maintenance agréés sont habilités à le faire.

Toute ouverture du boîtier du Firewall NETASQ par vos soins entraîne l'annulation de la garantie.

Une étiquette de garantie protège tous les appliances NETASQ contre l'ouverture du boîtier. La rupture de cette étiquette de garantie entraîne l'annulation de la garantie.

Les capots

Les capots NETASQ contiennent des ouïes de ventilation. Veillez à ne pas obstruer ces ouïes afin de ne pas altérer la circulation d'air à l'intérieur de celui-ci.

Des pieds caoutchoutés sont disposés sous le capot, assurant au Firewall NETASQ une très bonne stabilité (sur un bureau ou sur un autre équipement informatique).

© Copyright NETASQ 2006

Chapitre II

Installation, Pré-configuration, Intégration

© Copyright NETASQ 2006

Section A

Interface Graphique

© Copyright NETASQ 2006

La configuration du Firewall NETASQ se fait par un logiciel développé par la société NETASQ : le Firewall Manager. A partir de ce logiciel vous pourrez configurer entièrement votre firewall depuis un poste Windows.

L'installation de ce logiciel requiert les éléments suivants :

- ► PC Pentium III,
- ► 128 Mo de RAM (256 Mo conseillés),
- ► 100 Mo de disque dur,
- ► Carte réseau Ethernet 10 ou 100 Mbps,
- ► Windows Internet Explorer 5,
- ► Windows 2000 (SP3), XP (SP1).

NETASQ garantit le bon fonctionnement de sa suite logicielle, uniquement si celle-ci est installée sur un système d'exploitation Windows 2000 (SP3) ou Windows XP (SP1).

Pour cette section, vous devez

Posséder le fichier d'installation de l'interface graphique. Ce fichier est disponible sur le CD-ROM livré avec votre firewall ou sur le site WEB de NETASQ (www.netasq.com). Le fichier d'installation est bilingue.

Connaître l'adresse IP interne de votre firewall, ainsi que son numéro de série.

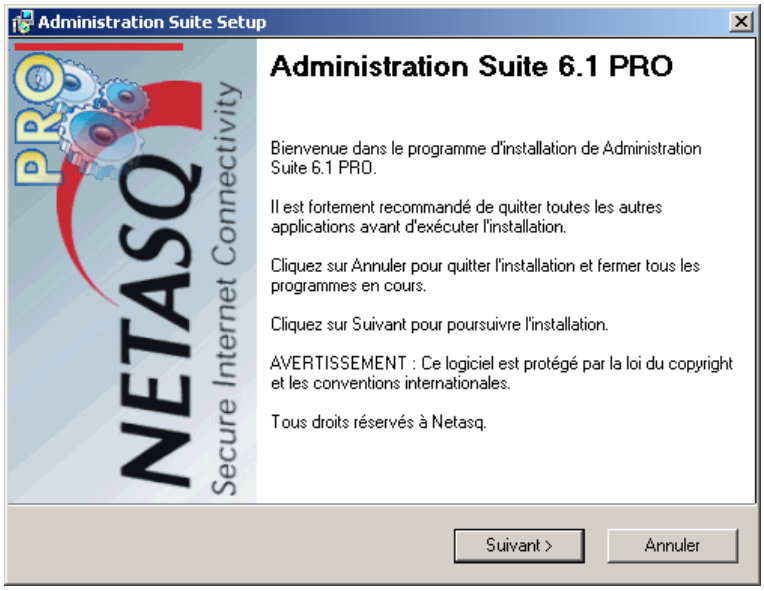
Utilité de la section

Cette section vous présentera les éléments pour l'installation et l'utilisation générale de l'interface graphique de configuration (Firewall Manager).

© Copyright NETASQ 2006

Procédure d'installation

Insérez le CD-ROM d'installation fourni ou téléchargez les fichiers nécessaires à partir du site Web NETASQ et exécutez le programme .EXE correspondant à la suite d'administration. Les informations d'installation apparaissent dans la langue de la version Windows.


Administration Suite Setup
Administration Suite 6.1 PRO
Bienvenue dans le programme d'installation de Administration Suite 6.1 PRO.
Il est fortement recommandé de quitter toutes les autres applications avant d'exécuter l'installation.
Cliquez sur Annuler pour quitter l'installation et fermer tous les programmes en cours.
Cliquez sur Suivant pour poursuivre l'installation.
AVERTISSEMENT : Ce logiciel est protégé par la loi du copyright et les conventions internationales.
Tous droits réservés à Netasq.
PRO
NETASQ
Secure Internet Connectivity
Suivant >
Annuler

Le logiciel d'installation suit le schéma d'installation "standard" d'une application sous Windows, c'est pourquoi il n'est pas décrit plus en détails dans ce manuel. L'installation typique n'inclut pas le NETASQ Syslog. Pour installer ce logiciel choisissez l'installation complète ou personnalisée.

Vous pouvez conserver, sur une même machine d'administration, l'interface graphique de plusieurs versions logicielles.

Quand le logiciel d'installation a terminé, vous disposez des programmes suivants dans le répertoire d'installation que vous avez choisi:

firewall.exe	Logiciel de configuration à distance du Firewall NETASQ et de consultation des traces.
monitor.exe	Module de réception en temps réel des alarmes générées par le Firewall NETASQ.
reporter.exe	Module de traitement des logs.

par défaut : "C:\Program Files\NETASQ\Administration Suite 5.0\"

Lors de l'installation, un enregistrement de votre produit vous est proposé. Cet enregistrement est obligatoire pour accéder au support technique NETASQ et pour récupérer la licence nécessaire à l'activation du boîtier. La section « Enregistrement » de ce manuel vous indique la marche à suivre pour cette étape de l'installation.

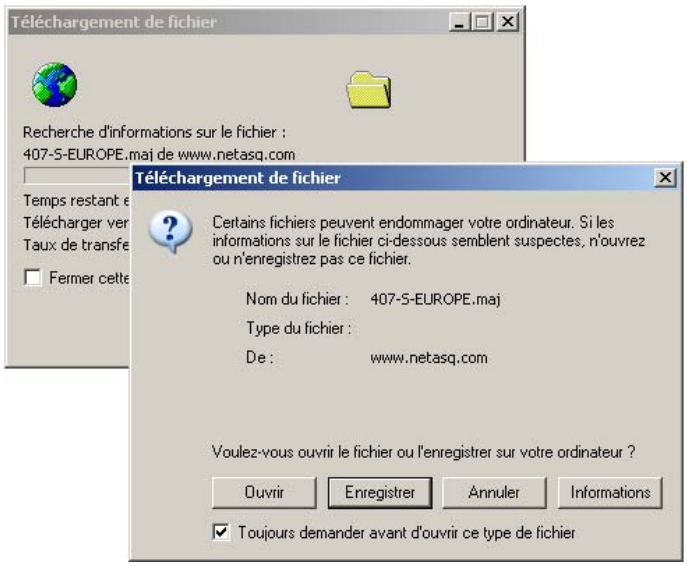
© Copyright NETASQ 2006

Les exécutables délivrés par NETASQ sont signés numériquement avec un certificat Thawte SA (Verisign). Cette opération assure l'origine et l'intégrité de l'application. En vérifiant la validité de la signature, vous aurez la certitude que le logiciel n'a pas été modifié ou échangé par un éventuel cracker.

Procédure de vérification de la signature

Pour vérifier la signature d'un fichier, veillez à ce que Internet Explorer, en version 4 minimum, soit installé sur votre poste.

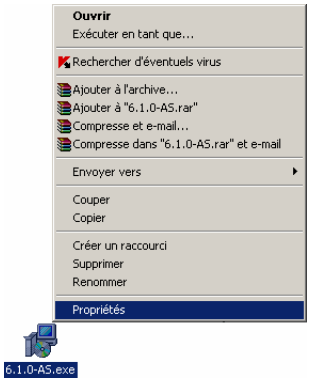
Lorsque vous téléchargez un applicatif à partir du site WEB de NETASQ, une fenêtre vous demande « Voulez vous ouvrir le fichier ou l'enregistrer sur votre ordinateur ? ».


Téléchargement de fichier
Recherche d'informations sur le fichier :
407-S-EUROPE.maj de www.netasq.com
Téléchargement de fichier
Certains fichiers peuvent endommager votre ordinateur. Si les informations sur le fichier ci-dessous semblent suspectes, n'ouvrez ou n'enregistrez pas ce fichier.
Nom du fichier : 407-S-EUROPE.maj
Type du fichier :
De : www.netasq.com
Voulez-vous ouvrir le fichier ou l'enregistrer sur votre ordinateur ?
Ouvrir
Enregistrer
Annuler
Informations
Toujours demander avant d'ouvrir ce type de fichier

► Si vous choisissez l'option « Ouvrir », votre explorateur WEB (Internet Explorer) réalisera automatiquement la vérification de la signature et vous en avisera.

► Si vous choisissez l'option « Enregistrer » (option recommandée), vous devrez réaliser la vérification manuellement.

Vérification manuelle



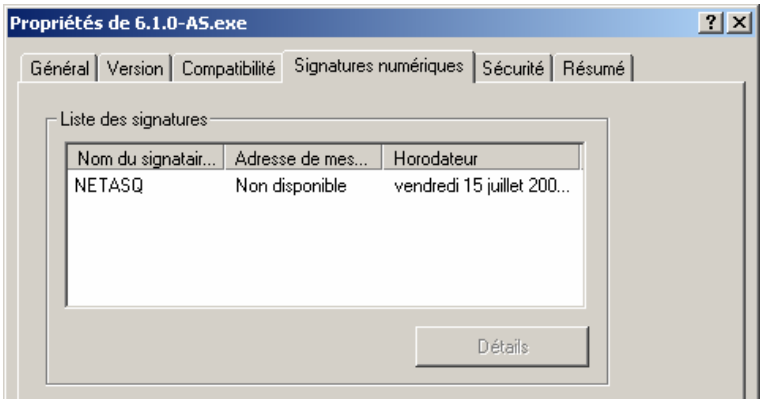
© Copyright NETASQ 2006

Pour effectuer la vérification manuelle de la signature de l'application, effectuez la procédure suivante avant d'installer l'applicatif :

1. Cliquez avec le bouton droit de souris sur l'application NETASQ dont vous voulez vérifier la signature, sélectionnez « Propriétés »,

2. Sélectionnez l'onglet « Signatures numériques » puis le nom du signataire (NETASQ),

3. Cliquez sur détails, la validité de la signature numérique est indiquée dans cette fenêtre.



Vous avez la possibilité de visualiser les informations du certificat ayant servi à signer l'application.

Lors de l'installation, un enregistrement de votre produit est proposé. Cet enregistrement est obligatoire pour obtenir la licence de votre produit, pour télécharger les mises à jour et pour accéder au support technique NETASQ. Si vous ne vous êtes pas enregistré à l'installation, vous avez la possibilité de le faire dans l'interface graphique de configuration NETASQ : le Firewall Manager.

Pour effectuer l'enregistrement de votre produit, suivez la procédure suivante :

1. Démarrez l'application NETASQ,

2. Sélectionnez le sous menu « ? > Enregistrement… » (il n'est pas nécessaire de vous connecter),

3. Un assistant d'enregistrement de vote produit vous propose deux types d'enregistrement, cliquez sur l'option qui vous correspond le mieux.

© Copyright NETASQ 2006

Section B

L’IPS-Firewall NETASQ

© Copyright NETASQ 2006

Pour cette section, vous devez avoir pris connaissance des sections suivantes

► Généralités,
► Interface graphique.

Pour cette section, vous devez connaître

► L'adresse IP de votre firewall (si le produit est encore en configuration usine, l'adresse IP est : 10.0.0.254).

Utilité de la section

Nous vous conseillons de prendre le temps de lire soigneusement ce manuel avant l'installation. Il vous aidera à vous familiariser rapidement avec l'appliance et les outils afférents. Cette première lecture vous familiarisera déjà avec l'IPS-Firewall NETASQ.

Un firewall est une pièce maîtresse dans votre réseau, ne le négligez pas : installez-le au mieux, dans les meilleures conditions.

Cette section vous permet de réaliser l'installation du boîtier et sa pré-configuration afin de l'intégrer dans l'architecture réseau désirée.

© Copyright NETASQ 2006

Préparation à l'installation physique du boitier

Précautions d'installation

Local d'installation

Le boîtier doit être installé dans un local fermé, ou à défaut une armoire verrouillée avec une protection physique d'accès. Tout accès non autorisé au boîtier risque de compromettre la sécurité de votre installation.

Recommandations d'installation

Les équipements lourds doivent être placés le plus bas possible dans le rack ou l'armoire et les équipements plus légers au dessus.

Assurez-vous que l'alimentation électrique est correctement reliée à une masse, correctement dimensionnée pour supporter l'alimentation du boîtier NETASQ et qu'elle est de préférence secourue par un onduleur.

N'installez pas le boîtier NETASQ dans un environnement dont la température ambiante dépasse les 35°C.

Assurez-vous que l'aération autour du produit peut être correctement réalisée et qu'aucun élément ne gêne la circulation d'air au travers des trous d'aération du produit.

Garantie

N'ouvrez jamais le boîtier. L'ouverture non autorisée du boîtier entraîne l'annulation de la garantie.

Préparation avant l'installation

Préparation des câbles réseau

Vous devez utiliser un câble réseau par interface de l'IPS-Firewall connectée à votre infrastructure.

Type de câble réseau en fonction du port réseau

Type de port Ethernet	Type de câble	Connectique
Port 10/100M Ethernet	Pour un fonctionnement en 10Mbits/s : paire torsadée catégorie3, 4 ou 5. Pour un fonctionnement en 100Mbits/s : paire torsadée catégorie 5	RJ45 RJ45
Port 1000BT Gigabit Ethernet (câble cuivre)	Pour un fonctionnement en 100Mbits/s ou 1000Mbits/s : Paire torsadée catégorie 5 ou plus.	RJ45
Port 1000FX Gigabit Ethernet (câble fibre)	Câble fibre optique	LC

Type de câble réseau en fonction de l'équipement connecté

Equipement connecté à l'IPS-Firewall	Type de câble
Hub	Câble droit.
Switch	Câble droit.
Modem	Câble droit ou croisé. Consultez la documentation du modem pour connaître le type de câble à utiliser. Vous pouvez aussi connecter l'IPS-Firewall et le modem (selon le type de modem) via la liaison série en utilisant un câble série droit.
Routeur	Câble croisé ou droit, si le routeur intégre un hub.
Autre firewall	Câble croisé.
PC	Câble croisé.

Un câble croisé est livré avec l'IPS-Firewall NETASQ.

Préparation de l'armoire ou du rack

Vous devez prévoir un espace minimum dans votre armoire ou votre rack pour l'installation du boîtier NETASQ. En fonction du produit l'espace minimum nécessaire en hauteur est différent :

- ► F25 : 1U
- ► F50 : 1U
- ► F200 : 1U
- ► F500 : 1U
- ► F1000 : 2U
- ► F2000 : 4U
- ► F5000 : 4U

Veuillez prévoir un espace vertical minimum entre chaque élément de l'armoire ou du rack pour la circulation d'air.

Préparation de l'accès Internet

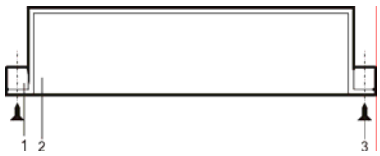
Avant l'installation de l'IPS-Firewall NETASQ, assurez-vous que les équipements d'accès à Internet (si l'IPS-Firewall doit être connecté avec le réseau Internet) ont été convenablement installés et configurés.

Tous les produits NETASQ peuvent être installés dans des armoires, baies ou rack 19 pouces. Les produits F1000, F2000 et F5000 intègrent des oreilles permettant l'installation directe du produit.

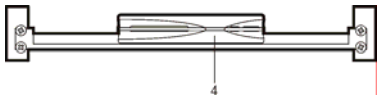
Les produits F200 et F500 sont livrés avec un système de fixation qui doit être ajouté au produit pour pouvoir installer celui-ci. Le système de fixation est disponible uniquement sur commande pour le F25 ou le F50.

Installation d'un F25 ou F50

Vue de dessus



Vue de face



1. Barres latérales de la baie
2. Plateau de support
3. Vis et écrous-cage
4. Produit

Un système de mise en baie peut être livré pour le F50 sur commande :

1. Installation du plateau sur la baie. Vissez le plateau de support sur les bords latéraux de la baie au moyen d'écrous-cage.

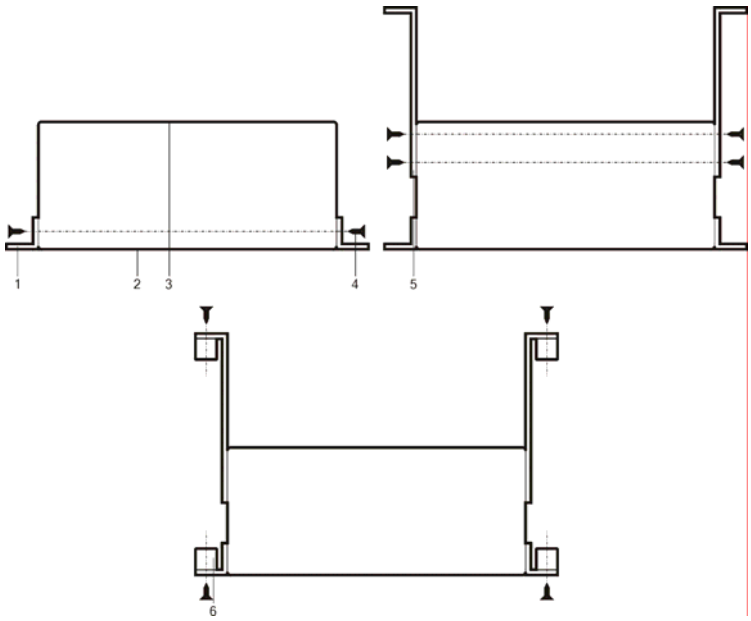
2. Une fois le plateau installé, vous pouvez déposer (aucune fixation n'est nécessaire) un ou deux produits sur le plateau de support.

Attention : prévoyez un espace d'1U au dessus du produit pour une bonne circulation des flux d'aération.

© Copyright NETASQ 2006

Installation d’un F200 ou d’un F500

F200 : Vue de dessus



1. Equerres
2. Face Avant
3. Face Arrière
4. Vis et écrous-cage
5. Barres de maintien
6. Barres latérales de la baie

Les F200 et F500 sont livrés avec un système d’équerres à fixer sur l’avant du boîtier et des barres de maintien latérales.

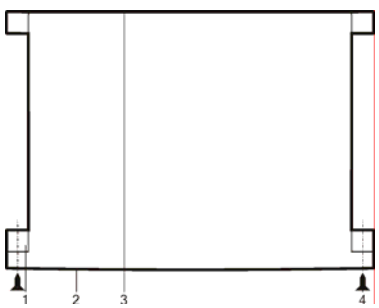
1. Mise en place des équerres de maintien. Vissez les équerres sur le boîtier. Les oreilles doivent être placées au niveau de la face avant du produit.

2. Mise en place des barres de maintien. Le positionnement des barres de maintien dépend de la taille de la baie.

3. Installation du boîtier dans la baie. Vissez les équerres et les barres de maintien sur les bords latéraux de la baie.

Installation d’un F1000, F2000 ou F5000

F1000 : Vue du dessus



© Copyright NETASQ 2006

1. Barres latérales de la baie
2. Face Avant
3. Face Arrière
4. Vis et écrous-cage

Le F1000, le F2000 et le F5000 disposent d'oreilles de fixation directement intégrées au chassis.

1. Installation du boîtier dans la baie. Vissez les oreilles de fixation du chassis sur les bords latéraux de la baie.

Les poignées métalliques présentes sur la face avant du produit ne doivent pas être utilisées pour porter celui-ci mais uniquement pour placer ou sortir l'appliance dans la baie.

Emplacement

Le Firewall NETASQ est prévu pour fonctionner en permanence, dans un bureau ou un local. Si vous ne possédez pas de baie de brassage, choisissez une surface plane et dégagée, évitez les endroits exposés à la chaleur (rayons du soleil par exemple), à l'humidité ou à la poussière.

Vous devez toujours veiller à protéger l'accès physique au boîtier (local ou armoire fermé à clé).

Raccordement de la prise secteur

Les IPS-Firewalls NETASQ peuvent fonctionner sur du 220V ou du 110V. Sur les modèles présentant un switch 110V/220V situé juste à côté de la prise femelle du Firewall, l'adaptation est manuelle (il faut placer le switch sur la valeur correspondant à votre installation électrique). Par défaut, ces boîtiers fonctionnent en 220V. Pour les autres modèles, l'adaptation se fait de manière automatique.

Insérez la prise femelle du cordon secteur fourni dans l'embase secteur mâle située sur la face arrière du boîtier NETASQ. Puis, enfichez la partie mâle du cordon secteur fourni dans une prise secteur adéquate.

Le Firewall démarre dès qu'il est relié au réseau électrique.

Une alimentation redondante est présente sur les IPS-Firewalls F1000, F2000 et F5000. Nous vous conseillons de raccorder chacune des alimentations sur une prise secteur différente pour vous prémunir de tous incidents électriques. De plus veillez à raccorder ces alimentations sur des onduleurs (« on line » de préférence).

Il est préférable d'utiliser une alimentation secourue par un onduleur.

Raccordement pour l'administration de l'appliance

L'administration de l'appliance s'effectue par défaut par l'intermédiaire de son interface INTERNE. Cette interface est suivant les modèles est identifiée par le chiffre 2 ou l'indication « IN » (F25 ou F50).

Raccordement au réseau

Reliez les différentes interfaces du Firewall aux éléments d'interconnexion réseau avec un câble RJ45. Les interfaces portent des numéros (voir au dos du produit) :

© Copyright NETASQ 2006

► L'interface identifiée « 1 » sur l'IPS-Firewall correspond à l'interface EXTERNE de l'IPS-Firewall (appelée OUT par défaut),
► L'interface identifiée « 2 » sur l'IPS-Firewall correspond à l'interface INTERNE de l'IPS-Firewall (appelée IN par défaut),
► Les interfaces indentifiées « 3, 4, 5, … » sur l'IPS-Firewall correspondent aux interfaces DMZ de l'IPS-Firewall (à l'instar de l'interface INTERNE, ces interfaces hébergent des réseaux internes).

Utilisation de câble droit

Un câble droit doit être utilisé entre un IPS-Firewall et un hub, un switch ou certains modems (selon le type de modem un câble droit ou croisé est nécessaire).

Utilisation de câble croisé (câble fourni avec le produit)

Un câble croisé doit être utilisé pour connecter l'IPS-Firewall à un élément actif de réseau (routeur, firewall, votre machine,certains modems...).

Attention, certains routeurs intègrent un hub, il faut donc dans ce cas utiliser un câble droit.

A la réception de votre IPS-Firewall NETASQ, celui-ci fonctionne en mode transparent et possède l'adresse IP 10.0.0.254 et le masque de sous réseau 255.0.0.0.

Ces paramètres ne correspondent pas à votre réseau, ils sont cependant nécessaires à la phase de pré-configuration.

Si vous ne savez pas ce que signifient ces paramètres, nous vous conseillons fortement de consulter un ouvrage sur TCP-IP car sans ce minimum de connaissances, la configuration de votre Firewall NETASQ sera difficile.

Voici les intervalles définis par les différentes classes d'adresses IP :

Classe	Plage d'adresses IP
A	0.0.0.0 à 127.255.255.255
B	128.0.0.0 à 191.255.255.255
C	192.0.0.0 à 223.255.255.255
D	224.0.0.0 à 239.255.255.255
E	240.0.0.0 à 247.255.255.255

Certaines parties de ces plages d'adresses sont réservées pour des réseaux privés :

Classe	Plage d'adresses IP réservées
A	10.0.0.0 à 10.255.255.255
B	172.16.0.0 à 172.31.255.255
C	192.168.0.0 à 192.168.255.255

Pré-configuration d'un poste Windows

La pré-configuration depuis un poste Windows est la méthode que nous vous conseillons. Nous allons utiliser un poste Windows. Ce poste peut être soit directement relié à l'interface interne de l'IPS-Firewall, soit connecté au réseau local, lui-même relié à l'interface interne de l'IPS-Firewall. Pour une connexion directe du poste sur l'IPS-Firewall, utilisez le câble croisé, livré avec le produit.

L'interface INTERNE de l'IPS-Firewall est appelée, sur le boîtier (face arrière), IN ou 2.

Pour vous connecter L'IPS-Firewall, vous devez utiliser un poste ayant une adresse IP dans le même sous-réseau que le IPS-Firewall, nous vous proposons d'utiliser l'adresse 10.0.0.1 et le masque réseau 255.0.0.0.

Pour configuer votre poste Windows veuillez suivre la procédure suivante :

1. Dirigez vous dans le « Panneau de configuration » de votre poste Windows,
2. Sélectionnez le menu « Réseau »,
3. Sélectionnez le protocole TCP/IP dans la liste des éléments réseau puis « Propriétés »,

© Copyright NETASQ 2006

4. Indiquez les informations d'adressage nécessaire à la configuration réseau du poste :

► Adresse IP : 10.0.0.250 ou l'adresse IP que vous avez choisie pour votre poste,
► Masque de sous réseau : 255.0.0.0,
► Passerelle par défaut : indiquez l'adresse actuelle de votre IPS-Firewall (10.0.0.254 par défaut).

Pré-configuration d'un IPS-Firewall

Vous pouvez désormais vous connecter à l'IPS-Firewall grâce à l'interface graphique de configuration NETASQ : le Firewall Manager.

Après avoir installé ce logiciel de configuration sur le poste client, vous pouvez modifier les paramètres des interfaces réseau de l'IPS-Firewall NETASQ pour l'adapter à vos adresses IP et choisir le mode de fonctionnement (transparent ou normal). Configuration réseau de l'IPS-Firewall

Si vous aviez changé l'adresse IP du poste client Windows pour faire cette configuration, n'oubliez pas de lui remettre son ancienne configuration.

Mécanisme Antispoofing

ATTENTION, si vous vous connectez à une interface puis débranchez le câble pour vous connecter sur une autre interface, vous déclencherez la sécurité anti-spoofing de l'IPS-Firewall (il est alors impossible de se connecter à l'appliance). Dans ce cas deux possibilités s'offrent soit vous modifiez l'adresse que vous venez d'attribuer à la machine d'administration (NETASQ recommande cette méthode) soit vous redémarrez l'appliance après avoir changé d'interface.

© Copyright NETASQ 2006

Section C

Première exécution

Pour cette section, vous devez avoir pris connaissance des section suivantes

► Interface graphique,
► Le firewall NETASQ.

Pour cette section, vous devez connaître

► L'adresse IP de votre firewall (si le produit est encore en configuration usine, l'adresse IP est : 10.0.0.254).

Utilité de la section

Les étapes décrites dans cette section vous accompagnent dans la découverte de votre IPS-Firewall NETASQ. Une fois que vous aurez pris en main l'interface graphique, vous serez en mesure de continuer la configuration de votre IPS-Firewall.

© Copyright NETASQ 2006

Le Firewall Manager, interface de configuration des IPS-Firewalls NETASQ peut être exécutée de plusieurs façons différentes.

Raccourci du menu démarrer

Suivez la procédure suivante pour démarrer l'interface depuis le raccourci du menu démarrer :

1. Cliquez sur le bouton « Démarrer » de votre bureau Windows,

2. Recherchez le menu dans lequel vous avez placé la Suite d'Administration NETASQ lors de l'installation (par défaut la section se nomme NETASQ),

3. Démarrez l'interface graphique NETASQ en cliquant sur le raccourci « Firewall Manager ».

Application « Firewall.exe » depuis le répertoire d'installation

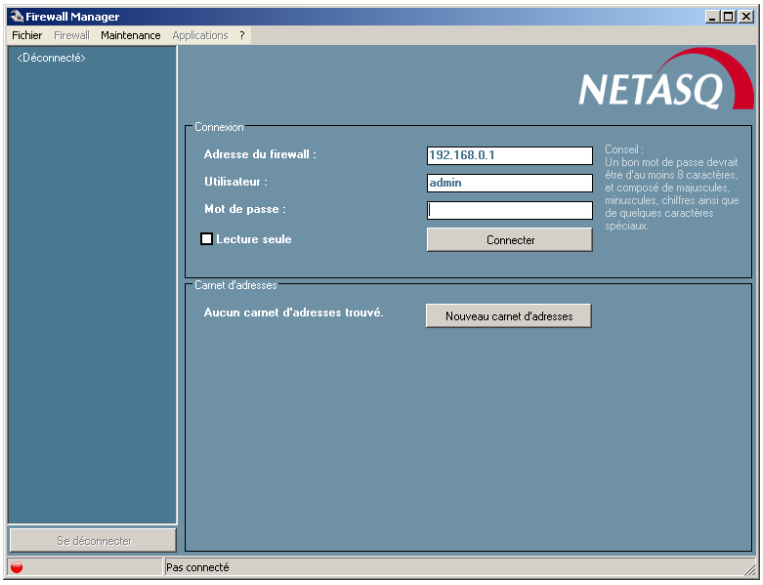
Suivez la procédure suivante pour démarrer l'interface depuis le répertoire d'installation :

1. Ouvrez votre explorateur de documents,

2. Recherchez le répertoire d'installation de la Suite d'Administration NETASQ (par défaut C:\Program Files\NETASQ\Administration Suite X.X),

3. Lancez le programme « Firewall.exe ».

Lorsque vous démarrez l'interface de configuration NETASQ, l'écran de démarrage de l'application vous rappelle la version du logiciel qui est installée. Puis la fenêtre principale de l'interface graphique de configuration des IPS-Firewalls NETASQ apparaît.



A partir de cette fenêtre, vous accédez aux différentes parties de la configuration des IPS-Firewalls NETASQ.

Tant que vous n'êtes pas connecté à un IPS-Firewall, vous ne pouvez accéder aux fonctionnalités principales de l'interface. Les menus auxquels vous avez accès sont :

► Le menu « Fichier » vous permet dans un premier temps de vous connecter à l'IPS-Firewall NETASQ. Il vous permet aussi d'accéder au sous-menu « Options » pour configurer différents paramètres. Reportez au chapitre « ACTIONS DIVERSES » pour plus d'informations.

© Copyright NETASQ 2006

► Le menu « ? » vous permet d'avoir accès aux fichiers d'aide et de connaître la version de l'interface graphique.

Une connexion d'administration à un IPS-Firewall s'effectue au moyen d'un logiciel de la suite d'administration NETASQ : Firewall Manager pour la configuration des fonctionnalités, Firewall Monitor pour le monitoring et Reporter pour l'aggrégation des traces et le reporting d'événements.

La configuration d'un IPS-Firewall n'est accessible qu'aux administrateurs du produit. NETASQ définit un administrateur par un utilisateur possédant des droits d'administration. L'attribution des droits aux utilisateurs est effectuée dans la configuration de cet utilisateur (voir la configuration des utilisateurs).

La première connexion

Par défaut, un appliance NETASQ n'est accessible qu'avec le Firewall Manager. Ce qui signifie que : TOUT ACCES AUTRE QUE LE FIREWALL MANAGER EST BLOQUE. Vous ne pouvez pas, par exemple, utiliser la commande PING pour vérifier le fonctionnement du boîtier.

Le compte « admin », super-administrateur

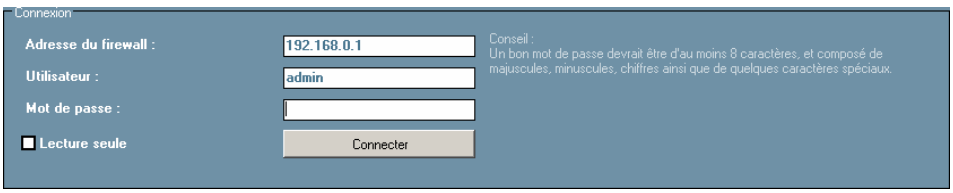
Par défaut, il n'existe qu'un seul utilisateur possédant des droits d'administration des produits NETASQ, le compte « admin » (son login est « admin »). Cet administrateur est un « super-administrateur ». Il possède tous les droits plus un droit spécial « ADMIN » qu'il est le seul à pouvoir posséder. Cela lui confère le droit effectuer certaines opérations comme attribuer des droits administratifs à un utilisateur par exemple. Sa configuration est impossible.

Etant donné les droits du compte « admin », NETASQ conseille de n'utiliser ce compte qu'en test ou dans le cas d'une maintenance. Ce compte est apparenté au compte « root » sous UNIX.

Processus de connexion

Le processus de connexion à un IPS-Firewall est défini par une procédure en trois étapes variables suivant l'avancement de la configuration (l'étape 3 n'est spécifique qu'à la première connexion par exemple).

Etape 1 : Envoi des informations de connexion à l'IPS-Firewall


Connexion
Adresse du firewall :
192.168.0.1
Utilisateur :
admin
Mot de passe :
Lecture seule
Connecter
Conseil :
Un bon mot de passe devrait être d'au moins 8 caractères, et composé de majuscules, minuscules, chiffres ainsi que de quelques caractères spéciaux.

Dans le cas de la première connexion

S'il s'agit de la première connexion à cet IPS-Firewall, les informations de connexion sont les suivantes :

► Adresse : « 10.0.0.254 », adresse IP des IPS-Firewalls NETASQ en configuration par défaut,
► Utilisateur : « admin », seul administrateur défini en configuration par défaut,
► Mot de passe : PAS DE MOT DE PASSE (champ vide), un mot de passe générique est utilisé en configuration par défaut,
► Lecture seule : « Décochée », pour pouvoir effectuer les premières étapes de configuration.

Un mécanisme d'affichage d'astuces vous permet d'obtenir des informations précises sur chacun des champs survolés par votre souris.

Lorsque les informations de connexion sont renseignées, cliquez sur le bouton « Se connecter » pour envoyer les informations de connexion à l'IPS-Firewall. Puis passez à l'étape suivante.

Dans le cas d'une autre connexion

La connexion auprès d'un IPS-Firewall demande les informations de connexion suivantes :

► Adresse : Adresse IP ou nom de machine de l'IPS-Firewall NETASQ sur le réseau interne,
► Utilisateur : nom d'utilisateur pour la configuration,
► Mot de passe : mot de passe pour l'utilisateur,
► Lecture seule : connexion à l'IPS-Firewall en mode lecture uniquement.

Si vous indiquez un nom de machine dans le champ « Adresse », ce nom doit être ajouté dans vos tables DNS ou dans le fichier « c:\winnt\system32drivers\etc\hosts » de la machine d'administration.

Un mécanisme d'affichage d'astuces vous permet d'obtenir des informations précises sur chacun des champs survolés par votre souris.

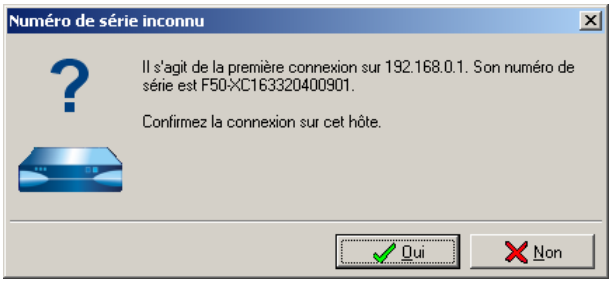
Attention, le Firewall NETASQ fait la différence entre les majuscules et les minuscules, aussi bien pour le nom d'utilisateur que pour le mot de passe.

Lorsque les informations de connexion sont renseignées, cliquez sur le bouton « Se connecter » pour envoyer les informations de connexion à l'IPS-Firewall. Puis passez à l'étape suivante.

Etape 2 : Validation du numéro de série de l'IPS-Firewall contacté

(étape réalisée uniquement lors de la première connexion à l'IPS-Firewall avec une station d'administration donnée)

Lors de la première connexion à l'IPS-Firewall avec une station d'administration donnée et que le numéro de série de l'IPS-Firewall contacté n'est pas renseigné dans le carnet d'adresses (voir configuration du carnet d'adresses) le Firewall Manager demande avant toute chose de valider le numéro de série de l'IPS-Firewall contacté.


Numéro de série inconnu
Il s'agit de la première connexion sur 192.168.0.1. Son numéro de série est F50-XC163320400901.
Confirmez la connexion sur cet hôte.
Oui
Non

La fenêtre apparue indique le numéro de série que l'IPS-Firewall (auprès duquel l'administrateur effectue une tentative de connexion) a renvoyé. Si le numéro de série ainsi affiché est identique à celui inscrit sur l'étiquette accolée sur le boîtier de l'IPS-Firewall, confirmez la connexion sur cet hôte en cliquant sur le bouton « Oui ». Puis passez à l'étape suivante. Sinon la connexion est interrompue.

Utilité de l'étape de connexion

Les sessions d'administration véhiculent des informations sensibles (mots de passe d'administration par exemple). Le détournement d'une telle session peut s'avérer désastreux pour la sécurité. En effet si un pirate s'empare d'un mot de passe administrateur, il peut modiier à sa guise la politique de sécurité de l'appliance.

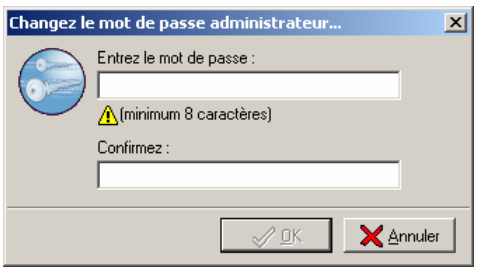
Chaque IPS-Firewall NETASQ est identifié par un certificat. Ainsi la validation du numéro de série de l'IPS-Firewall contacté permet d'éviter des attaques de type man in the middle.

Dans ce type d'attaque, le pirate s'insère entre la station d'administration et l'appliance. Il peut ainsi intercepter l'échange entre l'IPS-Firewall et l'administrateur. Bien que cette attaque soit très difficile à mettre en place, elle reste une menace identifiée, il est prudent de s'en prévenir.

Etape 3 : Enregistrement du mot de passe du compte « admin »

(étape réalisée uniquement lors de la première connexion à l'IPS-Firewall)

S'il s'agit de la première connexion à l'IPS-Firewall, le logiciel d'administration (Firewall Manager, Monitor ou Reporter) demande de définir un mot de passe indispensable pour le compte « admin ».



Spécifiez le mot de passe qui sera associé au compte « admin ». Cliquez sur Ok pour terminer le processus de connexion.

Notez que si ce message n'apparaît pas à votre première connexion, cela signifie que quelqu'un d'autre s'est connecté à votre produit avant vous. Contactez donc immédiatement votre partenaire.

Utilité de l'étape de connexion

Cette étape de connexion est un mécanisme de sécurité simple mis en place par NETASQ pour assurer l'intégrité de l'IPS-Firewall jusqu'à sa livraison. En effet :

► Cette étape est indispensable lors de la première connexion. Ainsi s'il s'agit de la première connexion et que cette étape n'apparaît pas cela signifie qu'une personne tierce a eu accès à l'appliance avant et que des modifications ont été effectuées.

► L'enregistrement du mot de passe du compte « admin », par le détenteur réel du compte « admin » permet de garantir l'entière confidentialité d'un mot de passe particulièrement sensible.

► La connexion à l'IPS-Firewall grâce à la console d'administration de l'appliance est impossible avant qu'un mot de passe de connexion valide soit défini. Avant la première connexion, le mot de passe de connexion « admin » ne peut être défini que par l'intermédiaire de l'interface graphique.

Restrictions d'administration

Droits d'administration

Chaque commande d'administration disponible sur un IPS-Firewall est associée à un droit de consultation / modification. Ceci se traduit par l'accès ou non à certains menus d'administration dans les logiciels d'administration de la suite NETASQ. Lorsqu'un administrateur est accrédité d'un droit donné, il est habilité à effectuer toutes les commandes associées à ce droit. La liste des droits disponibles sur les IPS-Firewalls est indiqué dans le Chapitre III Section B, la configuration des objets.

© Copyright NETASQ 2006

Multi-utilisation

Vous pouvez avoir un nombre illimité de sessions ouvertes simultanément avec des utilisateurs identiques ou différents. La seule contrainte est qu'à un moment donné vous ne pouvez avoir qu'une unique session avec les privilèges de modification « généraux » (pour éviter les conflits de modification). Ceci n'empêche pas d'autres utilisateurs de consulter la configuration, les utilisateurs possédant le droit MODIFY perdront temporairement ce droit si un utilisateur avec le droit MODIFY est déjà connecté.

Lorsqu'un administrateur est déjà connecté avec les privilèges de modification, un message vous indique que les privilèges de modification ont déjà été attribués et que vous pouvez choisir de récupérer ces droits ou de continuer la connexion sans droits de modification :

> Confirmation
>
> Vous avez perdu les privilèges de modification. Un utilisateur possédant ces privilèges est peut être déjà connecté. Voulez-vous récupérer les privilèges de modification (l'utilisateur connecté avec les droits de modification sera alors déconnecté) ?

La procédure permettant d'identifier l'utilisateur connecté avec les droits de modification est indiquée dans la section relative au Moniteur temps réel NETASQ.

Le carnet d'adresses

Le carnet d'adresses des logiciels NETASQ est un outil central dans la gestion des accès aux menus d'administration. En effet il peut contenir l'ensemble des informations de connexion nécessaires pour une connexion à une liste d'IPS-Firewalls, ainsi l'accès de l'administrateur est simplifié car il ne lui ai plus indispensable de retenir les mots de passe que cela implique.

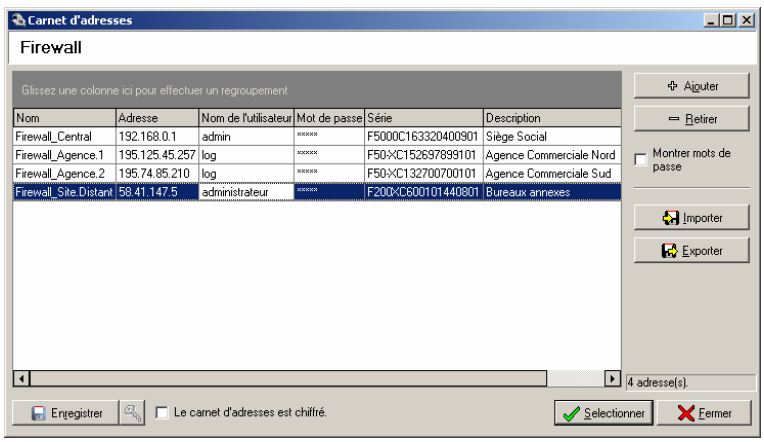
Pour des raisons de sécurité, le carnet d'adresses est spécifique à chaque machine d'administration (chaque installation de la suite d'administration possède son propre carnet d'adresses) mais commun aux trois applications qu'elle comprend (Firewall Manager, Monitor, Reporter). De plus il peut être chiffré.

Configuration du carnet d'adresses

Il existe deux façons d'accéder à la configuration du carnet d'adresses :

► Sur la page principale : cliquez sur le bouton « Nouveau carnet d'adresses » (lorsque celui-ci n'existe pas encore),
► Dans le menu Fichier>Carnet d'adresses.

Dans ce carnet d'adresses, il est possible de définir les IPS-Firewalls auxquels vous désirez vous connecter. Indiquez pour chaque IPS-Firewalls, un nom (ce champ est arbitraire et peut ne pas correspondre au nom de l'IPS-Firewall), une adresse IP, un mot de passe et un numéro de série.



Lorsque vous définissez un numéro de série pour un IPS-Firewall, ce numéro de série est ajouté à la liste des numéros de série connus la première fois que vous vous connectez à cet IPS-Firewall en utilisant le carnet d'adresses et cela sans qu'aucun message de confirmation n'apparaisse (étape 2 du processus de connexion).

Montrer les mots de passe

L'option « Montrer les mots de passe » permet d'afficher les mots de passe qui sont par défaut cachés dans le carnet d'adresses.

Importer et exporter

L'ensemble des informations présentées dans le carnet d'adresses peuvent être exportées pour servir par exemple à compléter un autre carnent d'adresses. Cliquez sur le bouton Exporter pour exporter les données et inversement cliquez sur Importer pour importer des données.

Le fichier d'importation des données doit respecter le formatage suivant :

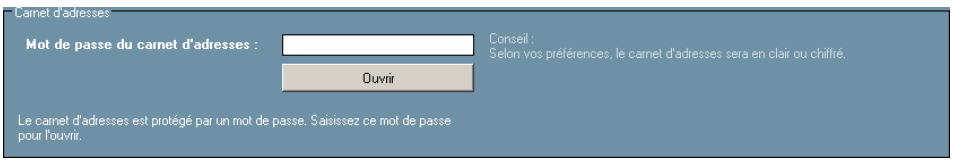
```
[BOOK]
Copyright=# Firewall Address Book (c)2001 NETASQ
AddressNumber=1

[1]
Name=Firewall_Central
Comment=Siège Social
Type=Firewall
Address=192.168.0.1
User=admin
Password=adminadmin
Serial=F5000C163320400901
```

Où

- ► Copyright : Obligatoire, a pour valeur « # Firewall Address Book (c)2001 NETASQ
- ► AddressNumber : nombre d'entrées dans le carnet d'adresses,
- ► [x] : sépare chaque ligne, x représente le numéro de ligne dans le carnet,
- ► Name : nom donné à l'IPS-Firewall dans la liste du carnet d'adresses,
- ► Comment : commentaire,
- ► Type : le type doit être obligatoirement « Firewall »
- ► Address : adresse de connexion à l'IPS-Firewall,
- ► User : login de l'administrateur,
- ► Password : mot de passe de l'administrateur,
- ► Serial : numéro de série de l'IPS-Firewall.

Le carnet d'adresses doit être chiffré

Pour des raisons évidentes de sécurité le carnet d'adresses peut être chiffré. Pour activer ce chiffrement, cochez l'option « le carnet d'adresses doit être chiffré » puis définissez le mot de passe associé. Ce mot de passe est indispensable à la lecture des informations contenues dans le carnet. Le chiffrement du carnet est effectué au moyen de l'algorithme AES, algorithme de chiffrement symétrique le plus performant actuellement.


Carnet d'adresses
Mot de passe du carnet d'adresses :
Ouvrir
Conseil :
Selon vos préférences, le carnet d'adresses sera en clair ou chiffré.
Le carnet d'adresses est protégé par un mot de passe. Saisissez ce mot de passe pour l'ouvrir.

Enregistrer

L'enregistrement des données ajoutées ou modifiées est indispensable avant toute fermeture du carnet d'adresses. Sinon toutes les modifications apportées sont perdues. Pour enregistrer les modifications du carnet d'adresses, cliquez sur le bouton « Enregistrer ».

Remarques

Les paramètres « Adresse » et « Utilisateur » saisis dans la boîte de dialogue de connexion sont sauvegardés dans la base de registres de votre PC d'administration. Pour des raisons évidentes de sécurité, le paramètre « Mot de passe » n'est pas sauvegardé.

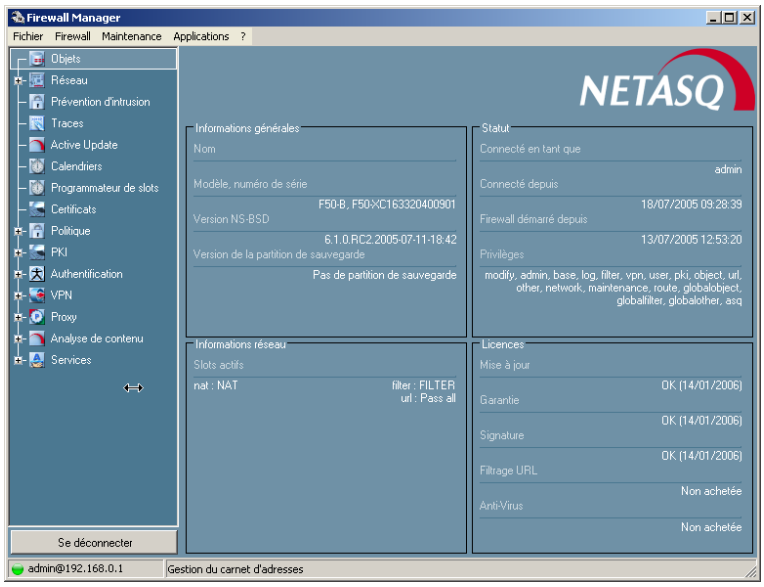
Fichiers du carnet d'adresses sur la machine d'administration

Sur la machine d'administration, les fichiers du carnet d'adresses se situent dans le repertoire d'installation de l'application. Il existe deux fichiers :

► AddrBook.dat : ce fichier contient le carnet d'adresses de la suite d'administration. S'il est chiffré les informations qu'il contient sont illisibles,
► AddrBook.srn : ce fichier contient la liste des numéros de série autorisés. Ce fichier n'est jamais chiffré.

© Copyright NETASQ 2006

Une fois connecté à l'IPS-Firewall, la fenêtre principale s'affiche. Les menus non accessibles au compte actuellement connecté sont inactifs.



La barre de menu

La barre de menu contient les entrées « Fichiers », « Configuration globale »,« Applications », « Firewall »" et « ? ».

Explication des menus

► **Fichiers :** connexion au firewall et déconnexion, édition du carnet d'adresses de firewall, édition de la liste de numéros de série de firewalls, sauvegardes et restaurations, options de l'interface graphique.

► **Configuration globale :** lorsque l'option (Voir « Affichage de la configuration globale ») et les droits de l'administrateur (Voir « droits d'administration ») le permet, ce menu s'affiche et permet d'accéder à la configuration globale des IPS-Firewalls.

► **Applications :** liens rapides avec les applications de la suite d'administration, le monitor et le reporter.

► **Firewall :** affichage des options de l'IPS-Firewall et gestion de la licence, configuration du système (date, heure, langue ...), configuration de la haute disponibilité, arrêt et redémarrage à distance du boîtier.

► **? :** accès aux fichiers d'aide, affichage de la boîte "A propos" indiquant le numéro de version de l'interface graphique, accès au formulaire d'enregistrement de produit.

L'arborescence

© Copyright NETASQ 2006

L'arborescence contient tous les menus de configuration des fonctionnalités des IPS-Firewalls. Lorsque le menu est grisé, la licence ou les droits de l'utilisateur ne permettent pas l'accès et/ou l'affichage de ce menu.

L'écran central

L'écran central est divisé en quatre sections distinctes :

► Informations

- ► Nom donné à l'IPS-Firewall,
- ► Modèle de boîtier,
- ► Version logicielle de l'IPS-Firewall (sur la partition principale) et numéro de série de l'IPS-Firewall,
- ► Version logicielle de la partition de Backup,

► Informations réseau

- ► Slots actifs à la connexion (filtrage, translation, VPN, etc),
- ► Des informations concernant la Haute Disponibilité.

► Statut

- ► Le compte utilisé pour la connexion,
- ► La durée écoulée depuis la connexion à l'IPS-Firewall,
- ► La durée écoulée depuis le démarrage de l'IPS-Firewall,
- ► Les droits accordés au compte utilisé pour la connexion.

► Licences

- ► La date d'expiration de l'option Mise à jour,
- ► La date d'expiration de la garantie,
- ► La date d'expiration de l'option « Signatures contextuelles »,
- ► La date d'expiration de l'option de filtrage de contenu.

Avant toute action ultérieure, vérifiez que la version logicielle de l'IPS-Firewall indiquée dans l'écran correspond bien à la version attendue. Il existe une seconde possibilité de vérifier la version du produit. Reportez vous Annexe H

La barre d'état

Dans le bas de la fenêtre principale se trouve la barre d'état composée de trois parties :

Voyant d'état	vous êtes actuellement connecté au Firewall NETASQ vous êtes déconnecté du Firewall NETASQ
Utilisateur@IP	nom de l'utilisateur connecté et l'adresse IP du firewall.
Zone de texte	Affiche le descriptif de l'action associée à une icône, le résultat d'une action ou le descriptif d'une erreur survenue.

Fermer la session

Pour vous déconnecter d'un IPS-Firewall, suivez la procédure suivante :

1. Sélectionnez le sous menu « Se Déconnecter » du menu « Fichier » dans les menus de l'interface de configuration ou cliquez le bouton

situé sous l'arborescence,

2. L'interface revient à l'écran principal.

Suivant les options définies par l'utilisateur (voir chapitre X), la déconnexion demande ou non une confirmation. L'annulation provoque le retour à l'écran principal, sans conséquence pour la suite de l'exécution du programme.

La déconnexion vous fait revenir à l'écran principal, mais le voyant d'état (en bas à gauche) est devenu : .

© Copyright NETASQ 2006

Section D

Intégration

Les firewalls NETASQ se caractérisent par une grande facilité d'intégration. Les quelques exemples d'architectures suivants le montrent.

Installation du firewall au sein d'une architecture déjà déployée

Le réseau que vous devez protéger par un firewall NETASQ est déjà connecté à Internet via un routeur dont vous n'assurez pas l'administration. Toutes les adresses IP du réseau interne ont déjà été configurées.

Solution NETASQ : insérez le firewall NETASQ entre le routeur et le LAN, en mode transparent (même adresse IP sur toutes les interfaces). Ainsi vous n'aurez à modifier ni l'adresse interne du routeur, ni les adresses IP de vos postes internes.

Installation du firewall au sein d'une architecture reposant sur une segmentation VLAN

Vous pouvez placer le firewall NETASQ en terminaison de VLANs ethernet. Le firewall pourra assurer le filtrage et le routage entre VLANs.

Installation du firewall derrière un modem

Vous installez un firewall NETASQ derrière un accès Internet modem (ADSL, RNIS, RTC ou modem câble) sans posséder de routeur.

Solution NETASQ : le firewall NETASQ peut gérer les connexions avec les modems de type ADSL (PPTP et PPPoE), RNIS, RTC et modem câble. Il n'est donc plus nécessaire d'avoir un routeur, le firewall peut sans problème le supplanter.

Migration d'un serveur du LAN vers la DMZ

Vous désirez mettre à disposition, sur Internet, un serveur qui n'était utilisé auparavant qu'à usage interne. Ce serveur était initialement placé dans votre réseau interne et vous souhaitez le déplacer dans la DMZ afin de l'isoler. Ce serveur possède une adresse IP privée appartenant à la classe d'adresses du réseau interne et il est difficile de changer cette adresse car les applications des postes internes sont configurées pour accéder au serveur par cette adresse.

Solution NETASQ : le firewall peut être configuré en mode hybride. Les interfaces du réseau interne et de la DMZ auront la même adresse IP, donc les machines reliées à ces deux interfaces seront considérées comme faisant partie du même réseau. Mais les flux entre le réseau interne et la DMZ seront filtrés. Vous pouvez alors déplacer le serveur vers la DMZ sans modifier son adresse IP.

Remarque : L'interface externe du firewall pourra avoir une adresse IP appartenant à un plan d'adressage différent (public ou privé).

© Copyright NETASQ 2006

Chapitre III

Configuration Réseau, Objets et ASQ

© Copyright NETASQ 2006

Section A

Configuration réseau

© Copyright NETASQ 2006

Pour cette section, vous devez avoir franchi les étapes

► Installation, pré-configuration, intégration.

Pour cette section, vous devez connaître

► Les paramètres IP à affecter au Firewall NETASQ pour chaque interface en cas de configuration avancée,
► L'adresse IP à affecter au Firewall NETASQ pour sa connexion au réseau en cas de configuration en mode transparent,
► L'adresse IP du routeur par défaut à utiliser,
► Les routes statiques en cas de fonctionnement routeur,
► Les paramètres de connexion, donnés par votre fournisseur d'accès, dans le cas d'un accès modem (RTC, RNIS, ADSL, modem câble).

Utilité de la section

Cette section vous permet de reconfigurer à distance les paramètres associés aux cartes réseau du NETASQ Firewall, ainsi que l'adresse IP du routeur par défaut.
Le Firewall peut fonctionner suivant deux modes :

► Mode bridge : il s'insère dans un réseau et possède une adresse située sur ce réseau. Avec ce mode vous n'avez pas besoin de modifier la topologie de votre réseau (passerelle par défaut, routes statiques,...). Le firewall fonctionne alors comme une passerelle,

►Mode avancé : vous séparez votre réseau en deux ou trois ou plus (selon le nombre d'interfaces que vous possédez) et affectez des adresses réseau différentes à chacune de ces parties. Cela vous permet de distinguer clairement les différentes parties de votre réseau au niveau adressage.

Accéder à cette section

Accédez à la configuration réseau par le « Réseaux **»** de l'arborescence.

Vous devez être connecté avec le droit « réseau » et les privilèges de modifications pour pouvoir effectuer des modifications sur la configuration des interfaces et le droit « routage » et les privilèges de modification pour pouvoir effectuer des modifications sur la configuration du routage.

Avant d'effectuer toute modification importante sur votre IPS-Firewall NETASQ, nous vous conseillons d'effectuer une sauvegarde (Voir « Sauvegarde »). Ainsi, en cas de mauvaise manipulation vous pourrez vous retrouver dans l'état précédent.

© Copyright NETASQ 2006

Les menus de configuration réseau permettent de configurer l'ensemble des paramètres réseau de l'IPS-Firewall, c'est-à-dire:

- ► le mode de fonctionnement des interfaces (bridge ou avancé),
- ► la ou les adresses IP du firewall ainsi que le réseau sur lequel il est connecté,
- ► les connexions distantes sur le port série (modem),
- ► le routage que l'IPS-Firewall effectue.

Vous avez la possibilité de définir des interfaces virtuelles qui peuvent appartenir à des VLANs de votre réseau. Ainsi le firewall NETASQ peut gérer les VLANs de votre architecture. Voir la configuration des VLANs

Vous pouvez aussi effectuer du routage par interface : en fonction de l'interface sur laquelle est reçu un paquet par le firewall, ce paquet est renvoyé vers une passerelle différente.

Une fois l'ensemble de ces paramètres entré, il suffit d'envoyer la configuration au firewall par le bouton « Envoyer ».

La modification de certains de ces paramètres nécessite le redémarrage de l'IPS-Firewall. Toutefois lorsqu'il n'est pas nécessaire, il est quand même recommandé. Dans ce cas, un message vous préviendra avant l'envoi à l'IPS-Firewall.

© Copyright NETASQ 2006

Vous pouvez configurer le fonctionnement entre interfaces de l'IPS-Firewall suivant trois modes différents :

► mode avancé,
► mode transparent,
► mode hybride.

Mode Avancé

Avec ce mode de configuration, le firewall fonctionne comme un routeur entre ses différentes interfaces.

Cela implique certains changements d'adresses IP sur les routeurs ou serveurs lorsque vous les déplacez dans un réseau différent (derrière une interface du firewall différente).

Les avantages de ce mode sont :

► la possibilité de faire de la translation d'adresses d'une classe d'adresses vers une autre,

► seul le trafic passant d'une interface à l'autre traverse le Firewall (réseau interne vers Internet par exemple). Cela allège considérablement le Firewall et fournit de meilleurs temps de réponse,

► meilleure distinction des éléments appartenant à chaque zone (interne, externe et DMZ). La distinction se fait par les adresses IP qui sont différentes pour chaque zone. Cela permet d'avoir une vision plus claire des séparations et de la configuration à appliquer pour ces éléments. De plus, vous pouvez appliquer des règles globales sur une zone avec les objets « Réseau ».

Mode Bridge ou mode transparent

Le mode transparent, aussi appelé "bridge" en anglais, permet de conserver le même adressage entre les interfaces.

Il simule un pont filtrant, c'est-à-dire qu'il est traversé par l'ensemble du trafic du réseau.

Cependant, vous pouvez ensuite filtrer les flux qui le traversent suivant vos besoins et donc protéger telle ou telle partie du réseau.

Les avantages de ce mode sont multiples:

► facilité d'intégration du produit car pas de changement de la configuration des postes client (routeur par défaut, routes statiques...) et aucun changement d'adresse IP sur votre réseau,

► compatibilité avec IPX (réseau Novell), Netbios sous Netbeui, Appletalk,

► pas de translation d'adresses, donc gain de temps au niveau du traitement des paquets par le Firewall.

Ce mode est donc préconisé entre la zone externe et la/les DMZ. Il permet de conserver un adressage public sur la zone externe du firewall et les serveurs publics de la DMZ.

© Copyright NETASQ 2006

Mode hybride

Le mode hybride utilise les deux modes précédents de façon simultanée. Ce mode ne peut être employé que pour les produits NETASQ possédant plus de deux interfaces réseau. Vous pouvez définir plusieurs interfaces en mode transparent (par exemple : zone interne et DMZ ou zone externe et DMZ) et certaines interfaces dans un plan d'adressage différent. Ainsi vous avez une plus grande flexibilité dans l'intégration du produit.

Conclusion

Le choix d'un mode se fait uniquement au niveau de la configuration des interfaces réseau. La configuration du Firewall est ensuite la même pour tous les modes.

Au niveau sécurité, tous les modes de fonctionnement sont identiques. On filtre les mêmes choses et la détection d'attaques est identique.

La configuration des interfaces sur un IPS-Firewall est effectuée dans le sous-menu « Interfaces » du menu « Réseau » de l'arborescence des menus du Firewall Manager.

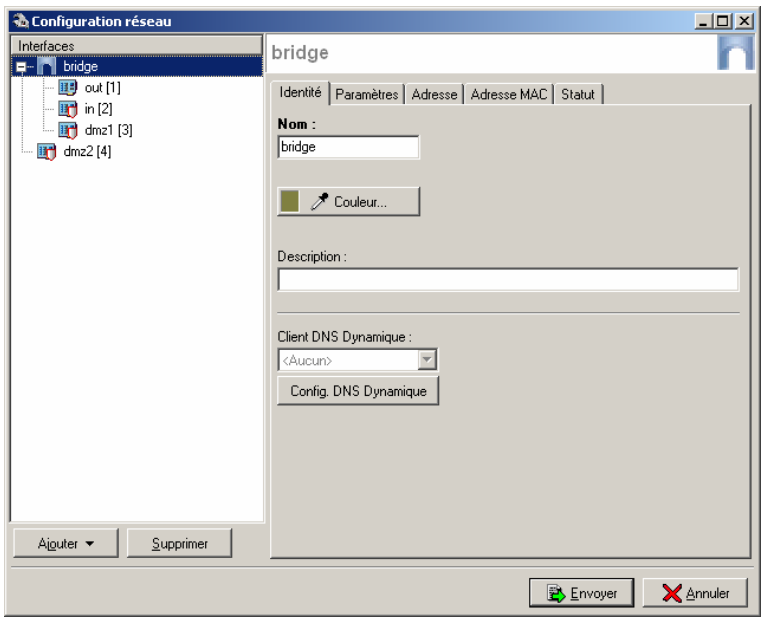
Elles peuvent être configurées de plusieurs façons :

► en transparent (bridge), les interfaces font partie du même plan d'adressage déclaré sur le bridge,

► en avancé, chaque interface possède une adresse IP différente et le réseau qui lui est relié fait partie de la même classe. Cela permet de configurer des règles de translation pour accéder à une autre zone du firewall,

► en mode hybride, certaines interfaces possèdent la même adresse IP et d'autres ont une adresse distincte.

Paramètres du Bridge



Pour modifier les paramètres d'un bridge, cliquez sur le bridge (identifié par l'icône) dans la partie gauche de la fenêtre. Quatre onglets permettent la modification des paramètres du bridge.

Onglet identité

Nom	Nom associé au pont. (voir la section Remarques pour connaître les noms interdits).
Couleur	Couleur attribuée à l'interface. Ces couleurs seront très utiles pour vous aider lors de la mise en place des règles de filtrage, des translations... En effet, chaque objet créé prendra une couleur en fonction de la zone à laquelle l'adresse IP appartient.
Description	Permet de donner un commentaire pour l'interface.

© Copyright NETASQ 2006

Client DNS dynamique	Lorsque votre IPS-Firewall ne possède d'adresse IP statique (son adresse IP est renouvelée régulièrement par votre fournisseur d'accès, DHCP, etc). Il est possible d'associer via un fournisseur de services DNS (dyndns.org par exemple) l'adresse IP allouée et un nom de domaine (qui lui est fixe) afin de pouvoir contacter cet IPS-Firewall sans pour autant connaître son adresse IP. Cette option vous permet d'activer cette fonctionnalité en sélectionnant un compte DNS dynamique vous avez préalablement configuré. La configuration des clients DNS dynamique est expliquée dans la suite du document (Voir « Configuration des clients DNS dynamique »).

Onglet Paramètres

MTU	Longueur maximale des paquets émis sur le support physique (Ethernet).
DHCP	Ce champ permet de spécifier au firewall que la configuration du bridge (adresse IP et masque) est définie par DHCP. Dans ce cas, l'onglet Adresse devient DHCP.

Onglet Adresse

Adresse	Adresse IP affectée au bridge. (Toutes les interfaces contenues dans le bridge possèdent la même adresse IP).
Masque réseau	Masque de réseau du sous-réseau auquel appartient le bridge. Les différentes interfaces faisant partie du bridge ont la même adresse IP donc tous les réseaux connectés au firewall font partie du même plan d'adressage. Le masque de réseau donne au firewall les informations sur le réseau dont il fait partie.
Description	Permet de spécifier un commentaire pour l'adressage du bridge.

Dans cet onglet, plusieurs adresses IP et masques associés peuvent être définis pour le même bridge (besoin de création d'alias par exemple). Ces alias peuvent vous permettre d'utiliser l'IPS-firewall NETASQ comme un point de routage central. De ce fait, un bridge peut être connecté à différents sous-réseaux ayant un adressage différent. Pour les ajouter ou les retirer, il suffit d'utiliser les boutons d'action (« Ajouter » et « Supprimer ») sous les champs Adresse IP et masque réseau.

Onglet Adresse MAC

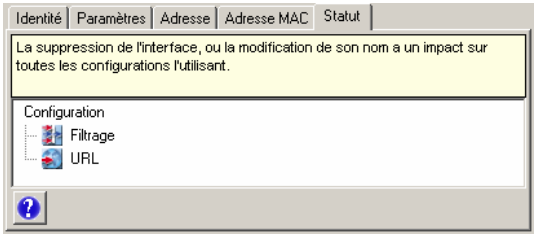
Cette option n'est pas accessible pour les IPS-Firewalls en haute disponibilité.

Cet écran vous permet de spécifier une adresse MAC pour une interface plutôt que d'utiliser l'adresse allouée par l'IPS-Firewall. Cela vous permet de faciliter d'autant plus l'intégration en mode transparent de votre IPS-firewall NETASQ dans votre réseau (en spécifiant l'adresse MAC de votre routeur plutôt que d'avoir à reconfigurer tous les postes utilisant cette adresse MAC).

Adresse MAC	Adresse MAC affectée au bridge. (Toutes les interfaces contenues dans le bridge possèdent alors la même adresse MAC).
Réinitialiser	Remise à zéro du champ Adresse MAC.

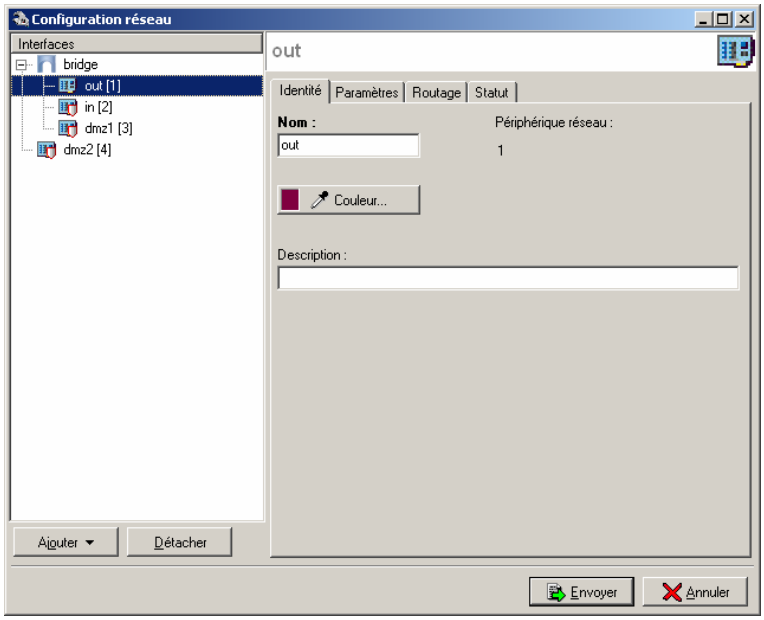
Onglet Statut

L'onglet Statut permet de visualiser les points d'utilisation de l'interface et de tous les objets et groupes d'objets générés par l'interface (Network_xx, Firewall_xx) dans la configuration de l'appliance UTM.



De plus en cliquant sur le bouton « », vous obtenez une visualisation plus précise de l'utilisation de l'interface, module par module, ligne par ligne.

Paramètres des interfaces du bridge



Vous pouvez modifier les paramètres de chaque interface appartenant au bridge. Pour cela, sélectionnez une interface située sous un bridge dans la partie gauche de la fenêtre. Trois onglets s'affichent alors :

Onglet identité

Nom	Nom associé à l'interface du pont. (voir la section Remarques pour connaître les noms interdits).
Couleur	**Couleur attribuée à l'interface**. Ces couleurs seront très utiles pour vous aider lors de la mise en place des règles de filtrage, des translations... En effet, chaque objet créé prendra une couleur en fonction de la zone à laquelle l'adresse IP appartient.
Description	Permet de donner un commentaire pour l'interface.

Onglet Paramètres

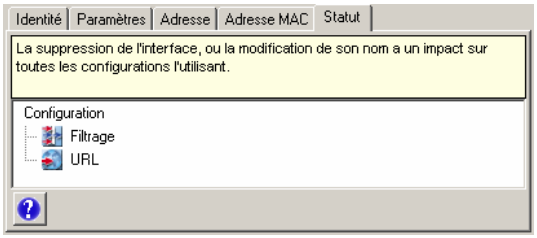
Activé	En cochant/décochant cette option on active/désactive l'interface. En désactivant une interface, on la rend inutilisable. En terme d'utilisation cela peut correspondre à une interface que l'on a prévu de déployer dans un futur proche ou éloigné mais qui n'est pas en activité. Une interface désactivée car non utilisée est une mesure de sécurité supplémentaire contre les intrusions.
MTU	Longueur maximale des paquets émis sur le support physique (Ethernet). Ce choix n'est pas disponible pour une interface contenue dans un bridge.
DHCP	L'adresse IP de l'interface est fournie par un serveur DHCP (utile pour les connexions Internet via le câble). (cf configuration de l'interface par DHCP). Ce choix n'est pas disponible pour une interface contenue dans un bridge.
Externe	Cochez cette option pour indiquer que cette partie du réseau est reliée à Internet. Dans la majorité des cas, l'interface externe, reliée à Internet, doit être en mode externe. Le caractère protégé de l'interface (matérialisé par un bouclier) disparaît lorsque cette option est cochée.
Privée	Cette option permet d'indiquer le caractère privé de l'interface. Les adresses des interfaces « privées » ne sont pas utilisables en tant que destination pour les paquets en provenance des interfaces non protégées, hormis si ceux-ci viennent d'être translatés. On notera que « privée » implique forcement d'être sur une interface protégée. Les options Externe et Privée sont donc incompatibles.
Média	Vitesse de liaison du réseau. Par défaut le Firewall le détecte automatiquement mais vous pouvez forcer l'utilisation d'un mode particulier. **Si l'IPS-Firewall est directement connecté à un modem ADSL, NETASQ vous recommande de forcer le média que vous voulez utiliser sur l'interface en question.**
Type	Cette option permet de définir quel type de machines est hébergé sur cette interface. Machine = machines de type hôte (utilisateurs), Serveur = machines de type serveur et inconnu = type de machine non défini. Ainsi, dans les traces, vous verrez quels types de flux (machine à machine, machine à serveurs …) transitent par le firewall.
Débit Informatif	En spécifiant le type de liaison Internet, il est possible de définir un débit maximal. Cette information n'est cependant pas utilisée pour réguler le trafic, elle définit l'échelle des graphiques du moniteur.

Onglet Routage

Passerelle	Permet de laisser passer les paquets IPX (réseau Novell), Netbios (sur NETBEUI), paquets AppleTalk (pour les machines Macintosh), PPPoE ou Ipv6 entre les interfaces du pont. Aucune analyse ou aucun filtrage de niveau supérieur n'est réalisé sur ces protocoles (le firewall bloque ou laisse passer).
Routage	Comme son nom l'indique l'option « Préserver le routage initial » permet de préserver le routage initial des machines connectées sur cette interface. Ainsi vous pouvez spécifier une passerelle par défaut pour certaines machines tout en spécifiant sur le firewall une passerelle pour celles qui n'en ont pas. Cette option facilite l'intégration du firewall dans une architecture composée de nombreuses passerelles différentes. Le champ « passerelle » sert au routage par interface. L'option « Garder les VLANs » permet la transmission des trames taggées sans que le firewall soit terminaison du VLAN. Le tag VLAN de ces trames sont conservées ainsi le IPS-Firewall peut être placé sur le chemin d'un VLAN sans pour autant que ce VLAN soit coupé par l'IPS-Firewall. L'IPS-Firewall agit de manière complètement transparente pour ce VLAN.
Passerelle locale	**Attention cette option n'est plus disponible dans la configuration réseau (Voir « Bypass ASQ »).**

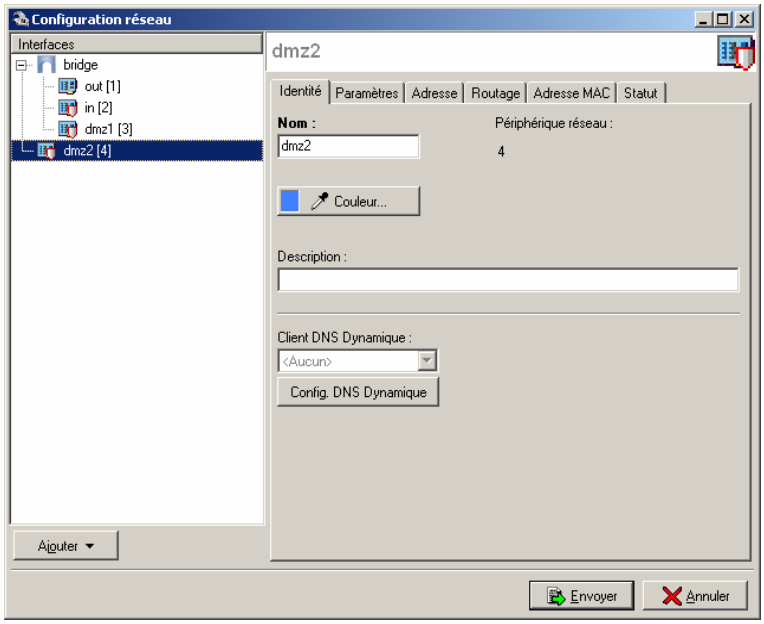
Onglet Statut

L'onglet Statut permet de visualiser les points d'utilisation de l'interface et de tous les objets et groupes d'objets générés par l'interface (Network_xx, Firewall_xx) dans la configuration de l'appliance UTM.



De plus en cliquant sur le bouton « », vous obtenez une visualisation plus précise de l'utilisation de l'interface, module par module, ligne par ligne.

Interface en mode avancé



Pour configurer une interface dans un réseau ne faisant pas partie d'un bridge, il suffit de la sortir de l'arborescence du bridge avec la souris ou en cliquant sur le bouton droit une fois l'interface sélectionnée (retirer du bridge). Vous pouvez ensuite configurer les paramètres de l'interface.

Onglet Identité

Nom	Nom que vous affectez à l'interface.(voir la section Remarques pour connaître les noms interdits).
Couleur	Couleur attribuée à l'interface. Ces couleurs seront très utiles pour vous aider lors de la mise en place des règles de filtrage, des translations... En effet, chaque objet créé prendra une couleur en fonction de la zone à laquelle l'adresse IP appartient.
Description	Commentaire associé à l'interface.
Client DNS dynamique	Lorsque votre IPS-Firewall ne possède pas d'adresse IP statique (son adresse IP est renouvelée régulièrement par votre fournisseur d'accès, DHCP, etc). Il est possible d'associer via un fournisseur de services DNS (dyndns.org par exemple) l'adresse IP allouée et un nom de domaine (qui lui est fixe) afin de pouvoir contacter cet IPS-Firewall sans pour autant connaître son adresse IP. Cette option vous permet d'activer cette fonctionnalité en sélectionnant un compte DNS dynamique vous avez préalablement configuré. La configuration des clients DNS dynamique est expliquée dans la suite du document (Voir « Configuration des clients DNS dynamique »).

Onglet Paramètres

Activé	En cochant/décochant cette option on active/désactive l'interface. En désactivant une interface, on la rend inutilisable. En terme d'utilisation cela peut correspondre à une interface que l'on a prévu de déployer dans un futur proche ou éloigné mais qui n'est pas en activité. Une interface désactivée car non utilisée est une

	mesure de sécurité supplémentaire contre les intrusions.
MTU	Longueur maximale des paquets émis sur le support physique (Ethernet).
DHCP	L'adresse IP de l'interface est fournie par un serveur DHCP (utile pour les connexions Internet via le câble). (cf configuration de l'interface par DHCP).
Externe	Cochez cette option pour indiquer que cette partie du réseau est reliée à Internet. Dans la majorité des cas, l'interface externe, reliée à Internet, doit être en mode externe. Le caractère protégé de l'interface (matérialisé par un bouclier) disparaît lorsque cette option est cochée
Privée	Cette option permet d'indiquer la caractère privée de l'interface. Les adresses des interfaces « privée » ne sont pas utilisables en tant que destination pour les paquets en provenance des interfaces non protégées, hormis si ceux-ci viennent d'être translatés. On notera que « privée » implique forcement d'être sur une interface protégée. Les options Externe et Privée sont donc incompatibles.
Média	Vitesse de liaison du réseau. Par défaut le Firewall le détecte automatiquement mais vous pouvez forcer l'utilisation d'un mode particulier. **Si le firewall est directement connecté à un modem ADSL, NETASQ vous recommande de forcer le média que vous voulez utiliser sur l'interface en question.**
Type	Cette option permet de définir quel type de machines est hébergé sur cette interface. Machine = machines de type hôte (utilisateurs), Serveur = machines de type serveur et inconnu = type de machine non défini. Ainsi, dans les traces, vous verrez quels types de flux (machine à machine, machine à serveurs ...) transitent par le firewall.
Débit Informatif	En spécifiant le type de liaison Internet, il est possible de définir un débit maximal. Cette information n'est cependant pas utilisée pour réguler le trafic, ce n'est qu'une indication.

Onglet Adresse (disponible si l'option DHCP n'est pas sélectionnée)

Adresse	Adresse IP affectée à l'interface.
Masque réseau	Masque de réseau du sous-réseau auquel appartient l'interface. Si l'option DHCP est sélectionnée, l'onglet adresse est remplacé par un onglet DHCP (voir section Configuration par DHCP).
Description	Permet de spécifier un commentaire pour l'adressage du bridge.

Onglet Adresse MAC

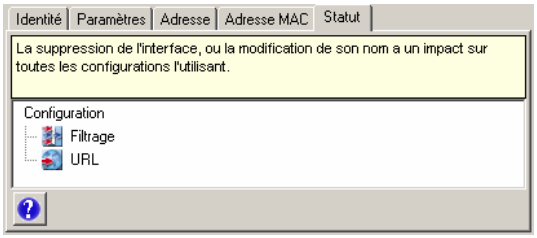
Adresse MAC	Adresse MAC affectée au bridge. (Toutes les interfaces contenues dans le bridge possèdent la même adresse MAC).
Réinitialiser	Remise à zéro du champ Adresse MAC.

Onglet Routage

Passerelle	Permet de laisser passer les paquets IPX (réseau Novell), Netbios (sur NETBEUI), paquets AppleTalk (pour les machines Macintosh), PPPoE ou Ipv6 entre les interfaces du pont.
Routage	Comme son nom l'indique l'option « Préserver le routage initial » permet de préserver le routage initial. Le champ « passerelle » sert au routage par interface. L'option « Garder les VLANs » permet la transmission des trames taggées sans que le firewall soit terminaison du VLAN. Le tag VLAN de ces trames sont conservées ainsi le IPS-Firewall peut être placé sur le chemin d'un VLAN sans pour autant que ce VLAN soit coupé par l'IPS-Firewall. L'IPS-Firewall agit de manière complètement transparente pour ce VLAN.
Passerelle locale	**Attention cette option n'est plus disponible dans la configuration réseau (Voir « Bypass ASQ »).**

Onglet Statut

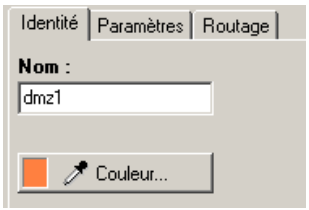
L'onglet Statut permet de visualiser les points d'utilisation de l'interface et de tous les objets et groupes d'objets générés par l'interface (Network_xx, Firewall_xx) dans la configuration de l'appliance UTM.



De plus en cliquant sur le bouton « », vous obtenez une visualisation plus précise de l'utilisation de l'interface, module par module, ligne par ligne.

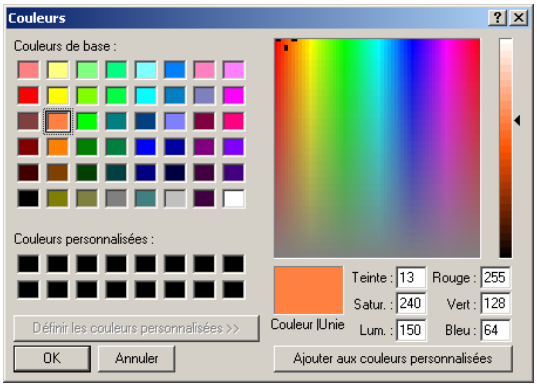
Définition des couleurs

Pour chaque interface définie dans la configuration réseau, une couleur peut être spécifiée. Tous les objets relatifs à une interface (machines ou réseaux) prendront la couleur définie pour cette interface.



La sélection d'une couleur est réalisée en cliquant sur le rectangle coloré situé sous le nom de l'interface. Une fenêtre s'affiche, vous avez alors la possibilité de choisir la couleur désirée parmi les couleurs prédéfinies ou définir vos propres couleurs (16 millions de couleurs).

© Copyright NETASQ 2006


Couleurs
Couleurs de base :
Couleurs personnalisées :
Définir les couleurs personnalisées >>
OK
Annuler
Couleur |Unie
Teinte : 13
Satur. : 240
Lum. : 150
Rouge : 255
Vert : 128
Bleu : 64
Ajouter aux couleurs personnalisées

Présentation des VLANs

Un réseau local (LAN) est basé sur le principe de diffusion. Chaque information émise par un équipement connecté sur le LAN est reçue par tous les autres.

Avec l'augmentation du nombre d'équipements raccordés sur le LAN, on aboutit à des situations de saturation. En effet, plus il y a de stations, plus il y a de risques de collisions.

Les réseaux virtuels (VLAN : Virtual Local Area Network) permettent de réaliser des réseaux axés sur l'organisation de l'entreprise. En effet, ils introduisent la notion de segmentation virtuelle, qui permet de constituer des sous-réseaux logiques étanches au sein même d'une architecture réseau. Les VLANs sont donc des regroupements logiques d'utilisateurs ou de stations (qui peuvent représenter l'organisation fonctionnelle de l'entreprise). Tous les membres d'un VLAN sont habilités à communiquer ensemble et forment un domaine de diffusion.

Les VLANs sont définis en fonction d'une marque (tag) des trames Ethernet (norme 802.1q).On peut ainsi définir des domaines de diffusion (domaines de broadcast). Les échanges à l'intérieur d'un domaine sont automatiquement sécurisés par l'étanchéité entre VLANs, et les communications inter domaines peuvent être contrôlées par une passerelle de niveau 3 comme un firewall.

Les IPS-Firewalls NETASQ peuvent se placer en terminaison de VLANs pour ajouter ou retirer un tag VLAN. Le firewall assure le filtrage entre VLANs et assure les communications entre les VLANS et les réseaux connectés aux autres interfaces du firewall.

Les VLANs sont perçus par le IPS-Firewall comme appartenant à des interfaces virtuelles, ce qui permet leur totale intégration au sein du système de sécurité de l'entreprise.

Avantage d'un VLAN

Le VLAN permet :

► Une augmentation des performances en limitant les domaines de diffusion,
► A un utilisateur qui déménage de retrouver les mêmes droits d'accès aux ressources LAN sans que l'exploitant n'ait eu à intervenir.

Définition des VLANs

Grâce à un IPS-Firewall NETASQ, il est possible de réaliser du VLAN de ports ou du bridge IP de VLANs.

Pour utiliser des interfaces VLAN sur l'IPS-Firewall vous devez obligatoirement posséder des équipements gérant les VLANs sur votre réseau (switchs ou commutateurs).

© Copyright NETASQ 2006

Suivez la procédure suivante pour définir des VLANs connectés à l'IPS-Firewall :

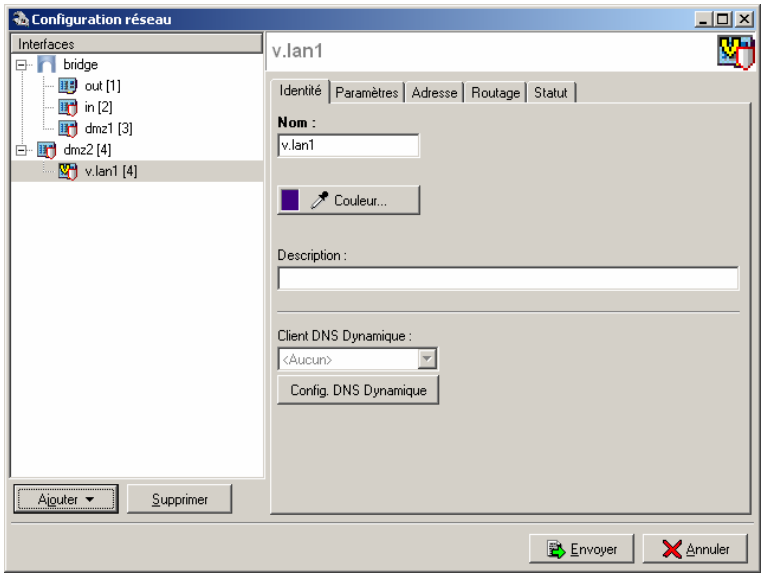
1. Sélectionnez le menu « Réseau » dans l'arborescence de l'interface de configuration,

2. Sélectionnez l'interface ou le bridge auquel vous désirez associer un VLAN,

3. Cliquez le bouton « Ajouter » et sélectionner « VLAN » ou cliquez avec le bouton droit de la souris et sélectionner « nouveau VLAN » dans le menu contextuel apparu.

Lorsqu'on développe le bouton « ajouter », l'interface sur laquelle on va insérer un VLAN est rappelée.

La configuration d'un VLAN est réalisée au moyen d'un assistant.



Les informations à spécifier dans l'assistant sont décrites dans les tableaux suivants.

Onglet Identité

Nom	Nom que vous affectez au VLAN.(voir la section Remarques pour connaître les noms interdits).
Couleur	Couleur attribuée au VLAN. Ces couleurs seront très utiles pour vous aider lors de la mise en place des règles de filtrage, des translations... En effet, chaque objet créé prendra une couleur en fonction de la zone à laquelle l'adresse IP appartient.
Description	Commentaire associé au VLAN.
Client DNS dynamique	Lorsque votre IPS-Firewall ne possède d'adresse IP statique (son adresse IP est renouvelée régulièrement par votre fournisseur d'accès, DHCP, etc). Il est possible d'associer via un fournisseur de services DNS (dyndns.org par exemple) l'adresse IP allouée et un nom de domaine (qui lui est fixe) afin de pouvoir contacter cet IPS-Firewall sans pour autant connaître son adresse IP. Cette option vous permet d'activer cette fonctionnalité en sélectionnant un compte DNS dynamique vous avez préalablement configuré. La configuration des clients DNS dynamique est expliquée dans la suite du document (Voir « Configuration des clients DNS dynamique »).

Onglet Paramètres

Activé	En cochant/décochant cette option on active/désactive l'interface. En désactivant une interface, on la rend inutilisable. En terme d'utilisation cela peut correspondre à une interface que l'on a prévu de déployer dans un futur proche ou éloigné mais qui n'est pas en activité. Une interface désactivée car non utilisée est une mesure de sécurité supplémentaire contre les intrusions.
Tag	Ce champ permet de spécifier quelle sera la valeur associée au VLAN dans les paquets transitant sur le réseau. Ce tag identifie le VLAN et est utilisé au niveau Ethernet.
MTU	Longueur maximale des paquets émis sur le support physique (Ethernet). Ce choix n'est pas disponible pour une interface contenue dans un bridge.
DHCP	L'adresse IP du VLAN est fournie par un serveur DHCP (utile pour les connexions Internet via le câble). (cf configuration de l'interface par DHCP). Ce choix n'est pas disponible pour une interface contenue dans un bridge.
Externe	Cochez cette option pour indiquer que cette partie du réseau est reliée à Internet. Dans la majorité des cas, l'interface externe, reliée à Internet, doit être en mode externe. Le caractère protégé de l'interface (matérialisé par un bouclier) disparaît lorsque cette option est cochée.
Privée	Cette option permet d'indiquer la caractère privée de l'interface. Les adresses des interfaces « privée » ne sont pas utilisable en tant que destination pour les paquets en provenance des interfaces non protégées, hormis si ceux-ci viennent d'être translatés. On notera que « privée » implique forcement d'être sur une interface protégée. Les options Externe et Private sont donc incompatibles.
Interface	Ce champ permet de définir physiquement quelle est l'interface de terminaison du VLAN.
Type	Cette option permet de définir quel type de machines est hébergé sur ce VLAN. Machine = machines de type hôte (utilisateurs), Serveur = machines de type serveur et inconnu = type de machine non défini. Ainsi, dans les logs, vous verrez quels types de flux (machine à machine, machine à serveurs ...) transitent par le firewall.
Débit informatif	En spécifiant le type de liaison Internet, il est possible de définir un débit maximal. Cette information n'est cependant pas utilisée pour réguler le trafic, ce n'est qu'une indication.

Onglet Adresse (disponible si l'option DHCP n'a pas été sélectionnée)

Adresse	Adresse IP affectée à l'interface VLAN.
Masque réseau	Masque de réseau du sous-réseau auquel appartient l'interface. Si l'option DHCP est sélectionnée, l'onglet adresse est remplacé par un onglet DHCP (voir section Configuration par DHCP).
Description	Permet de spécifier un commentaire pour l'adressage du bridge.

Cet onglet n'est bien sûr pas disponible pour un VLAN sur un bridge.

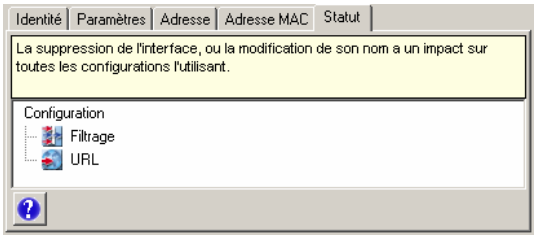
Onglet Routage

Passerelle	Permet de laisser passer les paquets IPX (réseau Novell), Netbios (sur NETBEUI), paquets AppleTalk (pour les machines Macintosh), PPPoE ou Ipv6 entre les interfaces du pont.
Routage	Comme son nom l'indique l'option « Préserver le routage initial » permet de préserver le routage initial. Le champ « passerelle » sert au routage par interface. L'option « Garder les VLANs » permet la transmission des trames taggées sans que le firewall soit terminaison du VLAN. Le tag VLAN de ces trames sont conservées ainsi le IPS-Firewall peut être placé sur le chemin d'un VLAN sans pour autant que ce VLAN soit coupé par l'IPS-Firewall. L'IPS-Firewall agit de manière complètement transparente pour ce VLAN.
Passerelle locale	**Attention cette option n'est plus disponible dans la configuration réseau (Voir « Bypass ASQ »).**

L'IPS-Firewall NETASQ réalise un filtrage au niveau IP, il faut donc associer à chaque VLAN, une adresse IP différente (l'IPS-Firewall maintient une table de correspondance entre un tag ethernet et une adresse IP. Lorsqu'un paquet provenant d'un VLAN arrive au firewall, le tag ethernet du VLAN sert à retrouver l'adresse IP qui sera utilisée dans les règles de filtrage).

Onglet Statut

L'onglet Statut permet de visualiser les points d'utilisation de l'interface et de tous les objets et groupes d'objets générés par l'interface (Network_xx, Firewall_xx) dans la configuration de l'appliance UTM.

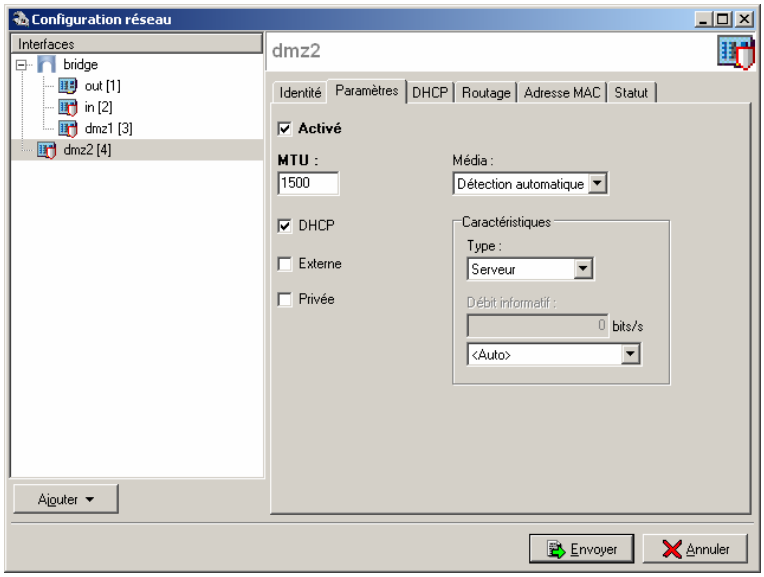


De plus en cliquant sur le bouton « », vous obtenez une visualisation plus précise de l'utilisation de l'interface, module par module, ligne par ligne.

VLAN dans un bridge

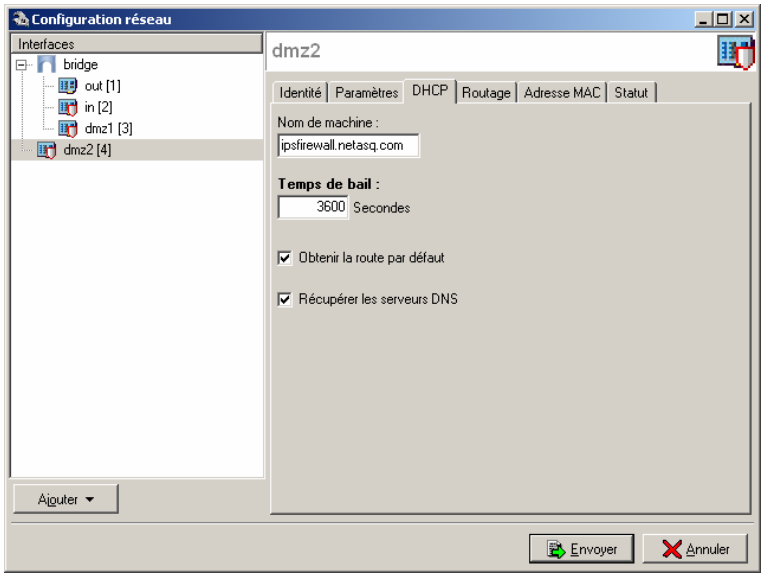
Dans la configuration des VLAN pour les bridges, il est possible d'utiliser le même tag pour deux interfaces VLAN associées à des interfaces physiques d'un même bridge. Ainsi l'IPS-Firewall apparaît de manière transparente sur le réseau. Cette méthode nécessite l'utilisation d'une interface VLAN par interface physique concernée.

Contrairement à l'option « Garder les VLAN » (qui rend l'IPS-Firewall complètement transparent par rapport au VLAN et qui empêche donc l'utilisation de fonctionnalités qui consisterait à couper le flux VLAN, par exemple les proxies), cette méthode de préservation du tag VLAN entre plusieurs interfaces d'un même bridge permet l'utilisation complète des fonctionnalités de l'IPS-Firewall.



L'IPS-Firewall est capable de récupérer l'adresse IP d'une de ses interfaces dynamiquement via un serveur DHCP externe. Ce cas de figure se présente pour une connexion Internet par **modem câble**.

Il suffit de cocher l'utilisation du DHCP dans l'onglet Paramètres. L'onglet DHCP apparaît à la place de l'onglet « Adresse ». Vous pouvez y indiquer les paramètres de la connexion DHCP :



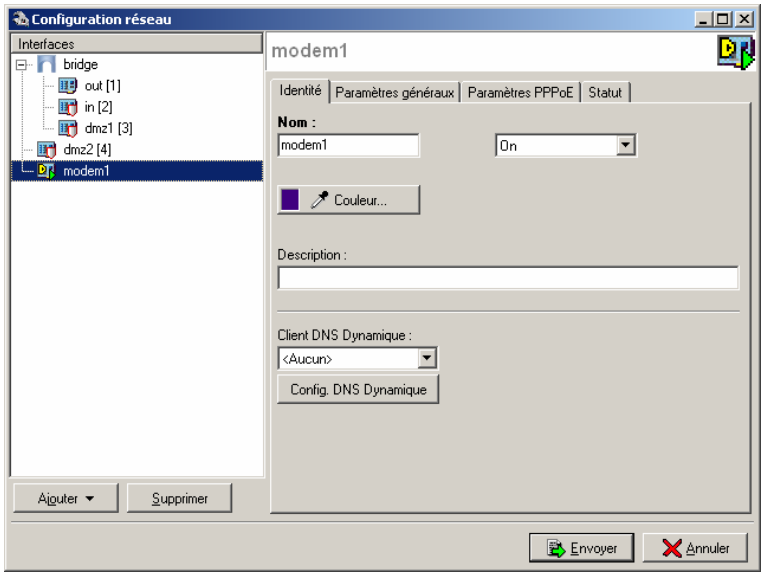
Nom de machine	Nom d'utilisateur (FQDN) pour la connexion. Ce champ facultatif, n'identifie pas le serveur DHCP mais l'IPS-Firewall. Si le champ est rempli et que le serveur DHCP externe possède l'option de mise à jour automatique du serveur DNS, alors le serveur DHCP met à jour automatiquement le serveur DNS avec le nom founi par l'IPS-Firewall et l'adresse IP qui lui a été fournie.
Temps alloué	Période de conservation de l'adresse IP avant re-négociation.
Route par défaut	Indique que l'interface en DHCP est connectée à la route par

© Copyright NETASQ 2006

	défaut de l'IPS-Firewall. Si cette option est cochée, l'IPS-Firewall reçoit sa route par défaut auprès du serveur DHCP (fournisseur d'accès par exemple). Elle remplace alors la route par défaut déjà configurée. Il est tout de même indispensable de configurer une route par défaut manuellement dans l'IPS-Firewall pour préserver la stabilité de l'appliance notamment dans la phase d'obtention de son adresse IP auprès du serveur DHCP.
Requête DNS	Lorsque cette option est cochée, l'IPS-Firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d'accès par exemple) qu'il contacte pour obtenir son adresse IP. Dès que cette option est cochée deux objets sont dynamiquement créés dans la base d'objets : Firewall_<nom de l'interface>_dns1 et Firewall_<nom de l'interface_dns2. Ils peuvent ainsi être utilisés dans la configuration du service DHCP. Ainsi si l'IPS-Firewall offre un service DHCP aux utilisateurs de son réseau, les utilisateurs seront crédités des serveurs DNS fournis par le fournisseur d'accès.

Dans ce cas, il faut utiliser l'objet « Firewall_out » dans les objets pour les configurations concernant l'interface externe.

Les interfaces dialup sont utilisées dans le cas de connexions distantes lorsque votre modem est branché directement sur le firewall (port série ou ethernet Out). L'IPS-Firewall accepte tout type de modem (ADSL, RNIS, RTC, ...) qui respecte le standard HAYES.



La création de nouvelles interfaces dialup (par défaut, il existe déjà les interfaces « dialup » et « atldialup ») se fait grâce à un assistant. Le nombre maximal de dialup disponibles sur votre firewall dépend du modèle.

Vous pouvez ensuite configurer les paramètres suivants de l'interface :

Onglet Identité

Nom	Nom que vous affectez à la connexion distante.(voir la section Remarques pour connaître les noms interdits).
Couleur	Couleur attribuée à la connexion distante. Ces couleurs seront très utiles pour vous aider lors de la mise en place des règles de filtrage, des translations... En effet, chaque objet créé prendra une couleur en fonction de la zone à laquelle l'adresse IP appartient.
Etat	Trois choix sont proposés. Off, par défaut, correspond à l'état inactif. ON correspond à l'état actif. Enfin Backup pour spécifier que cette interface n'est utilisé que lorsque les liens actifs ne sont plus opérationnels.
Description	Commentaire associé à la connexion distante.
Client DNS dynamique	Lorsque votre IPS-Firewall ne possède d'adresse IP statique (son adresse IP est renouvelée régulièrement par votre fournisseur d'accès, DHCP, etc). Il est possible d'associer via un fournisseur de services DNS (dyndns.org par exemple) l'adresse IP allouée et un nom de domaine (qui lui est fixe) afin de pouvoir contacter cet IPS-Firewall sans pour autant connaître son adresse IP. Cette option vous permet d'activer cette fonctionnalité en sélectionnant un compte DNS dynamique vous avez préalablement configuré. La configuration des clients DNS dynamique est expliquée dans la suite du document (Voir

	« Configuration des clients DNS dynamique »).

Deux connexions dialup (ou plus) peuvent être actives en même temps. Voir la section « Configuration de l'ASQ > Routage »

Onglet Paramètres Généraux

Login	Login chez le fournisseur d'accès.
Mot de passe	Mot de passe correspondant au login du fournisseur d'accès.
Type	Le type de connexion distante peut être PPP (RNIS, RTC), PPPoE (ADSL), PPTP (ADSL) ou L2TP.
Débit Maximum	En spécifiant le type de liaison Internet, il est possible de définir un débit maximal. Cette information n'est cependant pas utilisée pour réguler le trafic, ce n'est qu'une indication.
Route par défaut	Cette option définit l'interface dialup comme route par défaut de tous les paquets qui vont vers une adresse IP publique. Cette option est prioritaire sur l'option route par défaut de l'onglet « routage » du sujet suivant.
Mode	Le mode « Sur demande » n'établit la connexion avec Internet que lorsqu'une demande de connexion émane du réseau interne (ce mode est plus économique dans le cas d'une liaison payante à la durée). Le mode « Permanent » conserve la connexion vers l'Internet active en permanence.

Onglet Paramètres PPP (lorsque le type de connexion choisi est PPP)

Numéro de téléphone	Numéro d'appel chez le fournisseur d'accès.
Chaîne d'Initialisation	Chaîne de caractères servant optionnellement à initialiser la connexion.

Onglet Paramètres PPPoE (lorsque le type de connexion choisi est PPPoE)

Interface	Nom de l'interface sur laquelle est relié le modem ADSL.
Service	Type de service PPPoE utilisé. Cette option permet de différencier plusieurs modems ADSL. Par défaut, laissez ce champ vide.

Onglet Paramètres PPTP (lorsque le type de connexion choisi est PPTP)

Modem IP	Adresse IP interne du modem ADSL.

Onglet Paramètres L2TP (lorsque le type de connexion choisi est L2TP)

Les options de l'onglet « Paramètres L2TP » sont divisées en deux menus dont les paramètres sont expliqués ci-dessous.

Section « Général »

LNS	Adresse IP du serveur L2TP distant (LNS) utilisé pour la connexion L2TP.
Routeur pour l'accès LNS	La création d'une Dialup L2TP nécessite une route statique d'accès au serveur L2TP (LNS) définie par un routeur d'accès et

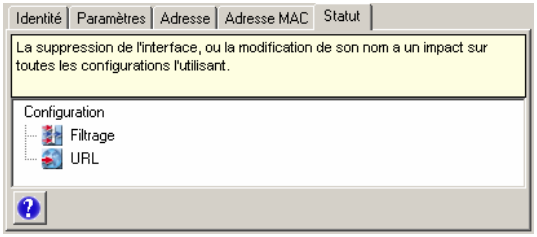
	l'interface à laquelle il est connecté. Cette option permet de définir le routeur d'accès.
Interface pour l'accès LNS	Nom de l'interface sur laquelle est relié le routeur LNS.
LNS secondaire	Dans le cas d'une défaillance du lien « principal » de la connexion L2TP, ce lien peut être secouru par une configuration secondaire. La configuration des options « secondaires » est identique au lien principal.

Section Avancé

Authentification du correspondant L2TP par secret partagé	L'authentification du client L2TP (ici l'appliance) sur le serveur s'effectue par défaut au moyen de son adressage IP. Lorsque cette option est cochée le client L2TP (ici l'appliance) propose au serveur une authentification par un secret partagé. Si le serveur accepte un secret partagé doit être échangé.
Protection des données sensibles (Hidden AVP)	Certaines données sensibles transitant dans le tunnel L2TP peuvent être protégées (masquage de mots de passe par exemple) lors de l'échange. Pour cela il est nécessaire de cocher l'option « Protection des données sensibles (Hidden AVP) » et de renseigner le secret partagé associé.
Secret partagé	Champ utilisé pour la définition du secret partagé indispensable aux options « Authentification du correspondant L2TP par secret partagé » et « Protection des données sensibles (Hidden AVP) ».
Expiration de reconnexion	Durée d'expiration en secondes d'une tentative de reconnexion du tunnel L2TP auprès du serveur L2TP distant (LNS).
Nombre de reconnexion	Nombre de tentative de reconnexion du tunnel L2TP auprès du serveur L2TP distant (LNS).
Utilisation du champ longueur dans les paquets L2TP	La RFC L2TP définit que l'utilisation du champ « longueur » des paquets L2TP soit facultative. Par défaut ce champ n'est donc pas utilisé mais dans le cas cela serait nécessaire (demande du serveur par exemple), cochez cette option.

Onglet Statut

L'onglet Statut permet de visualiser les points d'utilisation de l'interface et de tous les objets et groupes d'objets générés par l'interface (Network_xx, Firewall_xx) dans la configuration de l'appliance UTM.



De plus en cliquant sur le bouton « », vous obtenez une visualisation plus précise de l'utilisation de l'interface, module par module, ligne par ligne.

Remarques

► L'IPS-Firewall négocie automatiquement l'ouverture de ligne et réinitialise la connexion en cas de coupure. Dans le cas où la connexion n'est pas possible (problème de ligne), l'IPS-Firewall envoie un message d'alarme,

► L'IPS-Firewall crée un objet firewall_dialup représentant l'interface de connexion à Internet. Vous devez utiliser cet objet dans les règles de translation et de filtrage,

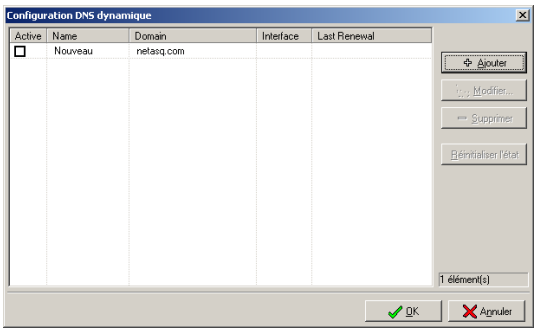
► Pour autoriser les connections PPTP, il faut aussi ajouter des règles de filtrage.

Introduction

Basé sur un échange entre un serveur (maintenu par un fournisseur de service DNS) et un client (intégré dans les IPS-Firewalls NETASQ), le service DNS dynamique permet d'associer vos IPS-Firewalls à un nom de domaine spécifique. Cela vous permet de pouvoir contacter ces IPS-Firewalls même si vous ne possédez pas d'adresse IP publique statique ou d'utiliser un nom de domaine simple à retenir plutôt qu'une adresse IP difficile à mémoriser.

Actuellement DynDNS.org est le seul fournisseur de service DNS supporté par les IPS-Firewalls. Contactez ce fournisseur pour obtenir un compte vous permettant la mise en place de ce service sur votre IPS-Firewall.

Fonctionnement



La configuration des clients DNS dynamique est accessible depuis la configuration des interfaces (bridge, interfaces en mode avancé, VLAN, Dialup).

Pour ajouter un client dans la liste des clients DNS dynamique configurés, cliquez sur le bouton « Ajouter ».

La configuration d'un client DNS dynamique est réalisée au moyen d'un assistant. Les informations à spécifier dans l'assistant sont décrites dans les tableaux suivants.

Configuration générale (Etape 1)

Nom de la configuration	Nom associé à la configuration du client DNS dynamique.
Nom de domaine	Nom de domaine attribué au client DNS dynamique. En utilisant l'option « use name wildcard », vous pouvez couvrir tous les sous domaine Par exemple si vous spécifiez « netasq.dyndns.org » dans le champ « nom de domaine » et que l'option « use name wildcard » est sélectionnée, tous les sous domaines (commerce.netasq.dyndns.org, labo.netasq.dyndns.org, etc) seront associés au client.

Fournisseur et configuration du compte (Etape 2)

© Copyright NETASQ 2006

Fournisseur dyndns	Fournisseur de services DNS. Actuellement, un seul fournisseur de services DNS est supporté : « DynDNS ».
Configuration du compte	Login et mot de passe indiqués par le fournisseur de services DNS pour l'authentification du client DNS dynamique.

Paramétrages DynDNS (Etape 3)

Service	Cette option vous permet d'indiquer le service que vous avez souscrit auprès de votre fournisseur de services DNS parmi « Custom DNS », « Dynamic DNS » et « Static DNS ».
Serveur	Serveur du fournisseur de services DNS. L'objet à spécifier dans ce champ doit obligatoirement se nommer : « members.dyndns.org » pour fonctionner avec DynDNS.

Dans l'étape 3, des paramètres de configuration avancée sont disponibles en cliquant sur le bouton « Paramètres Avancés ».

Renouvellement tous les (en jours) :	Période de renouvellement du service DNS dynamique. Cette période est fixée à 28 jours par défaut par NETASQ. Notez que DynDNS punit les renouvellements abusifs (fermeture du compte…). Ainsi un renouvellement survenu avant 26 jours (après le dernier renouvellement) n'est pas permis par DynDNS De plus sans renouvellement au delà de 35 jours, le compte est clôturé. Ces informations sont toutefois susceptibles d'être modifiées étant donné qu'il s'agit d'un fonctionnement établi par DynDNS.
Protocole	Protocole utilisé lors de la phase de renouvellement du service DNS dynamique.
Service hors connexion	Ce service, payant chez DynDNS permet de rediriger les flux à destination de votre réseau vers une page spécifique lorsque votre connexion n'est pas en activité.

Configuration du routage par interface

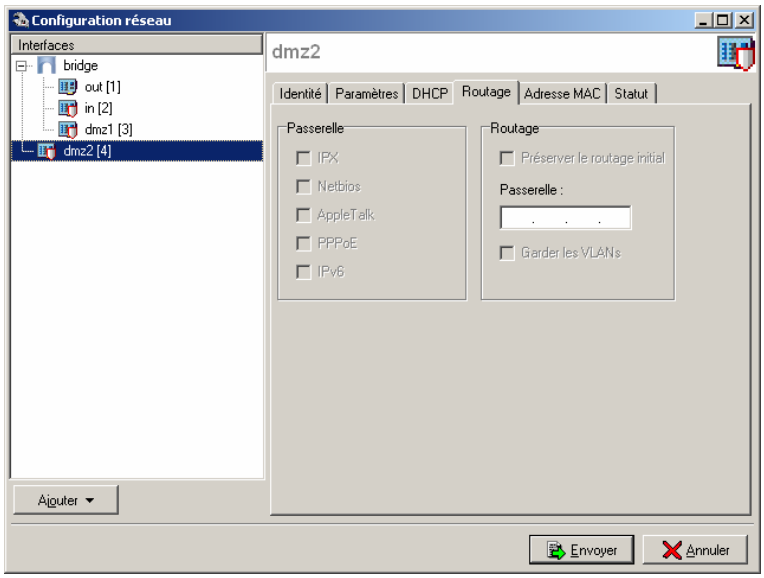
Certaines structures doivent pouvoir disposer de plusieurs accès Internet avec des caractéristiques bien spécifiques. Par exemple, une société hébergeant des serveurs publics sur son réseau doit pouvoir offrir une qualité de service optimale pour l'accès à ces serveurs. Parallèlement, elle doit donner à ses utilisateurs internes la possibilité d'accéder à Internet sans diminuer la bande passante dédiée aux serveurs publics. La fonctionnalité de routage par interface va permettre de définir, au niveau De l'IPS-Firewall, plusieurs accès Internet qui seront utilisés en fonction de l'interface sur laquelle arrive la demande de connexion. Il sera alors possible d'affecter un accès ADSL pour le réseau interne et une liaison spécialisée, avec garantie de service, pour l'accès à vos serveurs publics.

Configuration

Pour définir la configuration du routage par interface, veuillez vous reporter à la procédure suivante :

1. Choisissez l'onglet « Interfaces » de la fenêtre de configuration réseau,

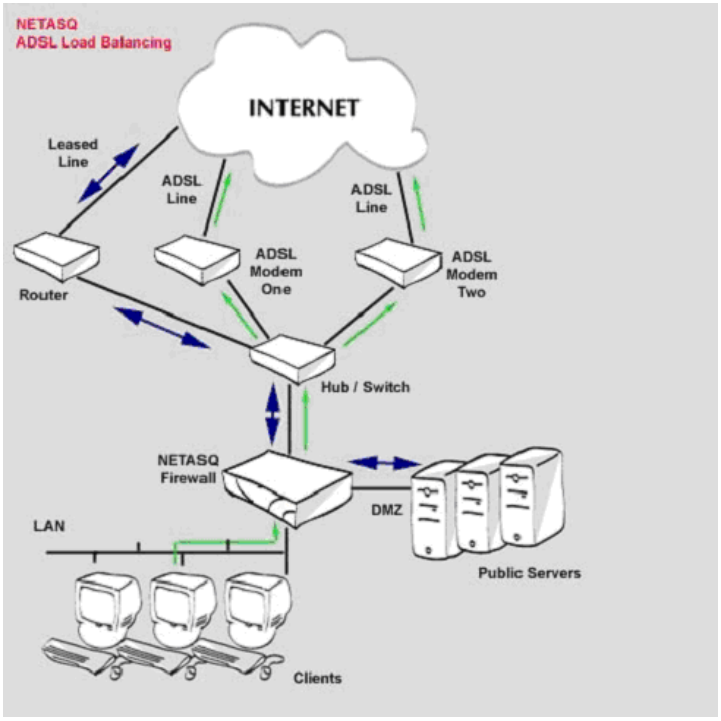
2. Choisissez l'interface désirée, puis l'onglet « Routage ».



Comme nous l'avons indiqué dans le sujet « Configuration des interfaces » pour chaque interface, vous avez un champ « Passerelle ». Ce champ doit renseigner l'adresse IP de la passerelle par défaut (passerelle pour la sortie Internet) utilisée lorsqu'une demande de connexion à destination de l'Internet arrive sur cette interface. Ce champ peut être laissé vide. Dans ce cas, la passerelle par défaut utilisée sera celle définie dans l'onglet « routage ».

Exemple d'architecture

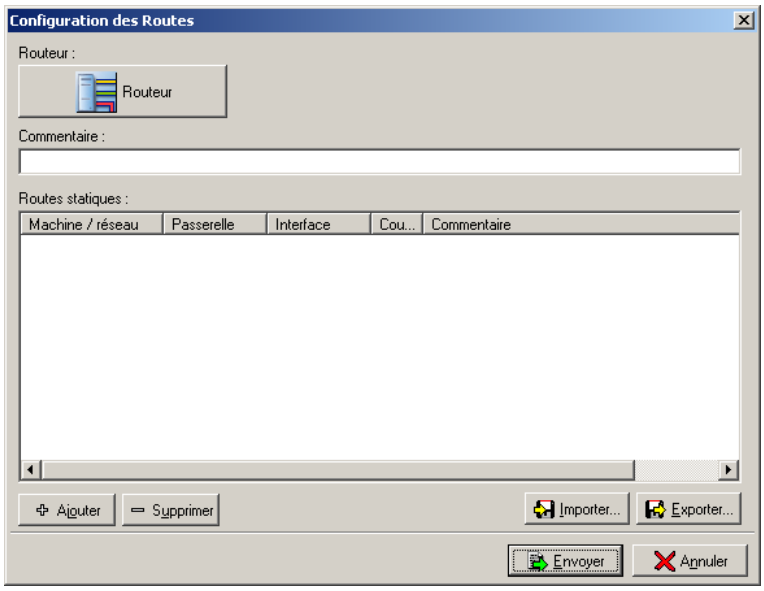
© Copyright NETASQ 2006



Dans cet exemple, l'accès ADSL a été doublé (pour un service de load-balancing d'accès).

Routeur par défaut et routes statiques

La configuration du routage sur un IPS-Firewall est effectuée dans le sous-menu « Routage » du menu « Réseau » de l'arborescence des menus du Firewall Manager.



Le menu « Routage » permet de configurer le routage effectué par le IPS-Firewall.

Routeur	Adresse IP du routeur par défaut. C'est à cette adresse que le Firewall NETASQ envoie les paquets qui doivent sortir sur le réseau public. Bien souvent le routeur par défaut est connecté à l'Internet.
Commentaire	Commentaires que vous pouvez saisir librement.
Routes statiques	Si vous possédez plusieurs réseaux "derrière" un routeur, vous pouvez spécifier ici les différentes routes. Vous sélectionnez alors un réseau ou un groupe d'hôtes puis la passerelle à utiliser pour atteindre ce réseau. Vous devez aussi préciser sur quelle interface est indirectement connectée cette passerelle. Vous pouvez ajouter ou retirer des routes statiques avec les boutons ajouter/supprimer.

Le routeur par défaut est généralement l'équipement qui permet l'accès de votre réseau à Internet.

Si vous ne configurez pas le routeur par défaut, l'IPS-Firewall NETASQ ne sait pas laisser passer les paquets possédant une adresse de destination différente de celles directement reliées au Firewall. Vous pourrez communiquer entre les machines sur les réseaux interne, externe ou DMZ, mais pas avec Internet.

Grâce aux boutons d'action disponibles au bas de la fenêtre, il est possible d'importer et d'exporter la configuration des routes statiques. Pour importer une configuration il faut respecter le format suivant :

RESEAU **,** INTERFACE **->** PASSERELLE **,** COULEUR **#** COMMENTAIRE

RESEAU : objet « réseau » correspondant au réseau distant
INTERFACE : interface sur laquelle se trouve la passerelle à utiliser pour atteindre le réseau
PASSERELLE : objet « machine » correspondant à la passerelle
COULEUR : couleur associée aux paquets provenant du réseau distant
COMMENTAIRE : commentaires que vous pouvez saisir librement

© Copyright NETASQ 2006

La modification des adresses IP interne et externe de l'IPS-Firewall NETASQ peut nécessiter des modifications importantes de vos fichiers de configuration afin qu'ils conservent leur cohérence. Avant de redémarrer l' IPS-Firewall NETASQ, n'hésitez pas à vérifier la cohérence de vos données, notamment dans les sections « Configuration des Objets », « Translation d'adresses » et « Filtrage ».

En aucun cas, une interface ne doit porter le nom « HA » ou un nom constitué de la façon suivante :

- « xx_peer" ou "firewall_yy ».
- xx étant le nom d'une interface déjà existante.
- yy étant une chaîne de caractères quelconque.

© Copyright NETASQ 2006

Section B

Configuration des objets

© Copyright NETASQ 2006

Pour cette section, vous devez avoir franchi les étapes

► Installation, pré-configuration, intégration,
► Configuration réseau.

Pour cette section, vous devez connaître

► Les machines et réseaux auxquels vous désirez affecter des droits particuliers,
► Les données sur les utilisateurs de votre réseau interne (nom, prénom ...),
► Les protocoles et les services IP que vous allez utiliser.

Utilité de la section

Cette section vous permet de définir les objets que vous allez utiliser pour la configuration de votre filtrage et de votre translation d'adresses. D'une part, vous donnez ici une correspondance entre un nom de machine, groupe de machines, réseau, groupe de réseaux et son adresse IP. D'autre part, vous donnez une correspondance entre un nom de service, son protocole et son numéro de port. Vous pouvez créer des groupes de services si certaines règles s'appliquent à plusieurs services. Vous pourrez aussi définir ici les comptes utilisateurs pour l'authentification. Les informations sur ces comptes sont stockées dans une base LDAP interne au firewall, mais peuvent aussi être stockées dans une base LDAP externe ou avec des informations limitées sur un serveur RADIUS ou une base Active Directory.

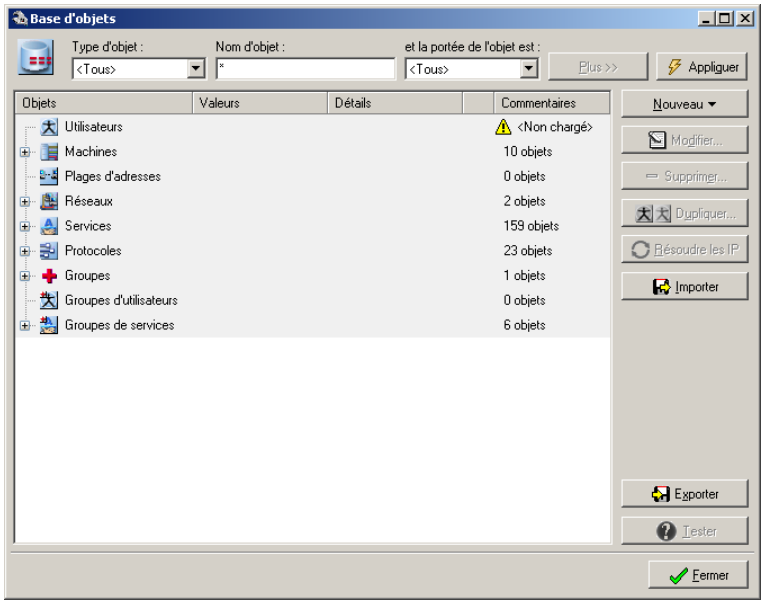
Accéder à cette section

Accédez à la boîte de dialogue par le menu « Objets » de l'arborescence.

Vous devez être connecté avec les privilèges de modification pour pouvoir effectuer ces modifications.

Avant d'effectuer toute modification importante sur votre IPS-Firewall NETASQ, nous vous conseillons d'effectuer une sauvegarde. Ainsi, en cas de mauvaise manipulation vous pourrez vous revenir dans la configuration précédente.

© Copyright NETASQ 2006



La fenêtre de définition des objets est divisée en trois parties :

- ► Une zone de tri et de sélection en haut de la fenêtre,
- ► Une barre d'action, sur la partie droite de la fenêtre,
- ► Une grille de définition des objets.

Zone de tri et de sélection

La zone de tri et de sélection située en haut de la fenêtre se présente différemment suivant le type d'objet actuellement sélectionné. A l'ouverture tous les objets sont listés dans la grille de définition des objets mais lorsqu'un SEUL type d'objet est sélectionné (menu déroulant situé en haut à gauche), la zone de tri et de sélection apparaît.

Cette zone de tri et sélection permet une recherche rapide d'un objet parmi la liste des objets configurés sur votre IPS-Firewall. Les champs de recherche de cette zone ne sont pas expliqués dans la suite du document tant ils sont intuitifs.

Les boutons d'actions

Cette zone contient un certains nombres de boutons d'actions qui vous permettent de valider et d'afficher votre recherche.

Type d'objet	Sélection du typr d'objet affiché parmi : « Tous », « Utilisateurs », « Machines », « plages d'adresses », « Réseaux », « Services », « Protocoles », « Groupes », « Groupes d'utilisateurs, « Groupes de réseaux ».
Nom de l'objet	Recherche d'un objet contenant la chaîne de caractères indiquée.
Plus / Moins	Affichage ou masquage de la zone de tri et sélection.
Appliquer	Appliquer la recherche

© Copyright NETASQ 2006

Caches les objets spéciaux	Les objets spéciaux sont les objets créés par défaut par l'IPS-Firewall et qui seront utilisés à l'activation des services associés (par exemple : Firewall_pptpXX, Firewall_dialupXX, Firewall_ipsec…). Ces objets rendent la lecture générale difficile et sont cachés par défaut.

La barre d'action

Les actions permises par la barre d'action sont indiquées dans le tableau suivant.

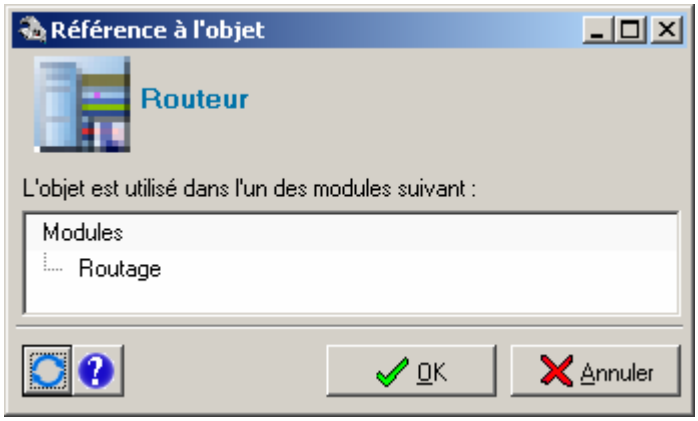
Nouveau	Choisissez le type d'objet que vous désirez créer et l'assistant de création correspondant apparaît.
Modifier	Modifier l'objet sélectionné.
Supprimer	Supprimer l'objet sélectionné.
Dupliquer	Dupliquer l'objet sélectionné.
Résolution de adresses IP des hôtes	Effectuer la résolution des adresses IP des hôtes de type « semi-dynamique ».
Importer	Importer une liste d'objets
Exporter	Exporter la liste des objets
Tester	Effectuer un test de l'utilisation de l'objet sélectionné. Voir « Références à l'objet ».
Fermer	Fermer la fenêtre de configuration des objets. Une modification sur un objet est automatiquement prise en compte.

Attention, l'importation d'objet ne dispose pas de mécanismes de protection pour assurer l'intégrité de la configuration importée (le fichier importé peut contenir des informations volontairement erronées). Il est donc de la responsabilité de l'administrateur de valider la cohérence de l'ensemble de la base objet importée avant son envoi sur l'IPS-Firewall.

De plus il n'est pas récommandé de faire des sauvegardes de la base objet par ce moyen, préférez pour cela les fonctions de sauvegarde de configuration (qui disposent de mécanismes cryptographiques).

Références à l'objet

Lorsqu'on clique sur le bouton « Tester » ou lorsqu'un objet (sauf utilisateurs) est supprimé de la base d'objets, un écran de référence à l'objet apparaît. Cet écran pointe les différents modules qui utilisent dans leur configuration l'objet sélectionné.



L'écran de référence à l'objet reprend en premier lieu le nom de l'objet puis indique, sous forme de liens directs, les différents modules dans lesquels l'objet est utilisé. Lorsqu'on clique sur un module listé par l'écran de référence, le menu de configuration associé est affiché permettant une visualisation et/ou une modification de la configuration avant suppression de l'objet.

L'écran de référence à l'objet possède une barre d'action constituée de quatre boutons d'actions :

	Actualiser l'affichage proposé par l'écran de référence à l'objet.
	Afficher le retour textuel exact de l'IPS-Firewall indiquant précisément dans chaque module l'endroit où est utilisé l'objet. Par exemple : module=Filter slot=10 line=1 module=Filter slot=10 line=2 module=Route section=Default
OK	Fermeture de l'écran référence de l'objet avec validation des changements.
Forcer	Le bouton OK de l'écran référence de l'objet devient Forcer lors de la suppression d'un objet. Cette action supprime l'objet sélectionné malgré son utilisation dans les modules cités.
Annuler	Fermeture de l'écran référence de l'objet sans validation des changements.

Les modifications réalisées par l'intermédiaire de l'écran de référence à l'objet, dans les modules utilisant l'objet analysé, ne peuvent pas être annulées par un click sur le bouton Annuler de l'écran.

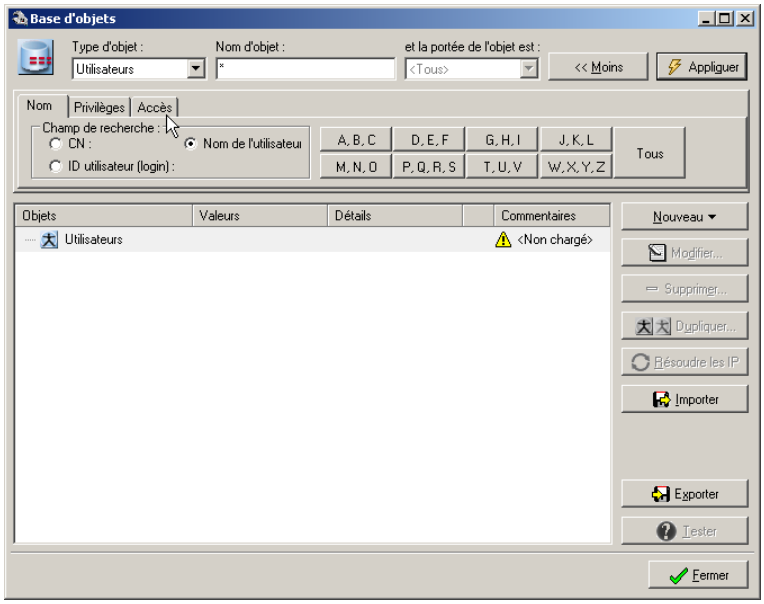
Remarques

Remarques : les objets prennent la couleur des interfaces dont ils dépendent. Toutes les modifications concernant les utilisateurs (LDAP) sont immédiatement appliquées.

Si un objet utilisé dans la configuration de l'appliance UTM est modifié, cette modification est automatiquement prise en compte par l'appliance UTM et les slots utilisant cet objet sont automatiquement réactivés.

Attention, la réactivation d'un slot de NAT entraîne la perte des connexions actives.

© Copyright NETASQ 2006



Le service d'authentification des utilisateurs nécessite la création de comptes utilisateurs au niveau de l'IPS-Firewall. Ces comptes contiennent l'ensemble des informations relatives à ces utilisateurs :

- nom,
- prénom,
- login de connexion,
- mot de passe,
- e-mail (optionnel),
- numéro de téléphone (optionnel),
- description (optionnel),
- méthode d'authentification de l'utilisateur,
- droits d'accès VPN et droits d'administration,
- clé pré-partagée pour le VPN,
- mot de passe PPTP,
- certificat x509.

Création d'un utilisateur

Assistant de création d'un utilisateur

La création d'un utilisateur (bouton « Nouveau » > « Utilisateur ») est réalisé au moyen d'un assistant. Cet assistant en une étape vous demande de renseigner les informations suivantes :

- Nom de la personne,
- Prénom de la personne,
- Nom d'utilisateur : login qui sera utilisé pour l'authentification de l'utilisateur,
- Email de la personne,
- Numéro de téléphone,
- Champ de description.

Attention, si vous désirez générer un certificat x509 pour cet utilisateur vous devez forcement indiquer son adresse mail. Cette information sera utilisée dans le certificat.

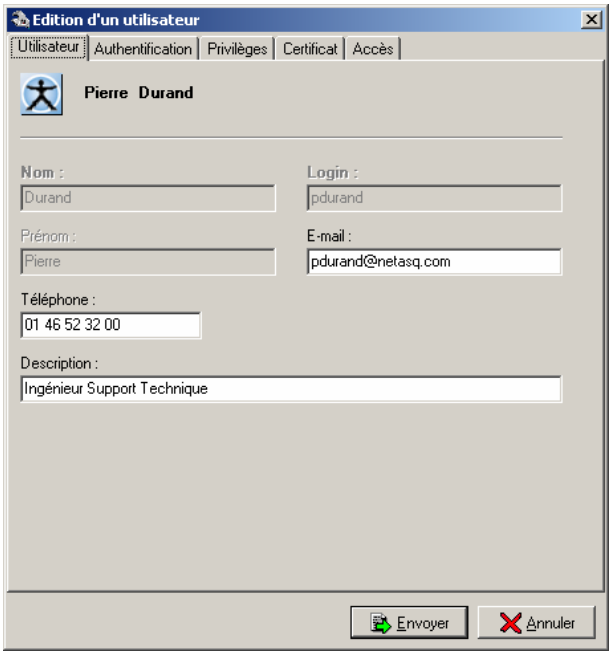
© Copyright NETASQ 2006

L'adresse mail est aussi nécessaire si l'utilisateur désire se connecter au firewall en VPN avec un client mobile IPSEC.

Une fois la configuration avec l'assistant effectuée ou lorsque vous souhaitez modifier la fiche d'un utilisateur (sélectionnez l'utilisateur dans la grille d'objets, puis cliquez sur le bouton « Modifier ») les informations relatives à la configuration de l'utilisateur sont affichées dans une fenêtre comportant cinq onglets.

Remarque : toutes les modifications concernant les utilisateurs sont immédiatement appliquées.

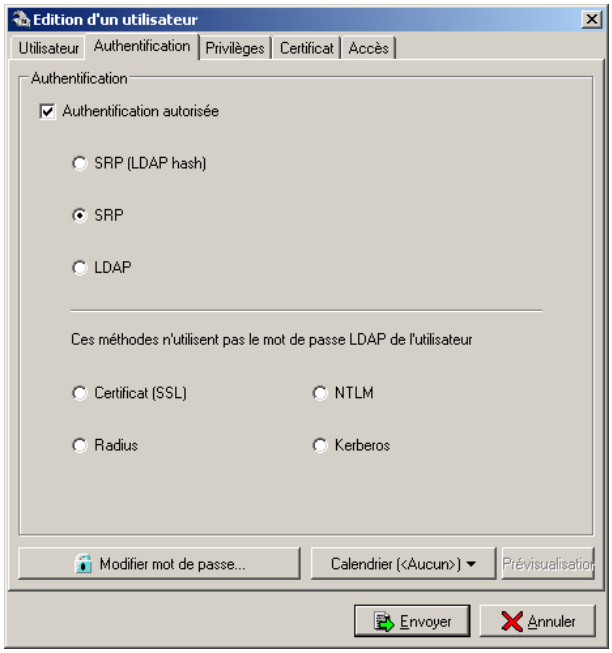
Onglet « Utilisateur »



Cet onglet permet de modifier les informations de base sur l'utilisateur :

- Nom de la personne,
- Prénom de la personne,
- Login de connexion, login qui sera utilisé pour l'authentification de l'utilisateur,
- Email (facultatif),
- Numéro de téléphone (facultatif),
- Description (facultatif).

Onglet « Authentification »



Cet onglet donne les éléments de configuration pour l'authentification :

► LDAP : le mot de passe transite non modifié dans un tunnel SSL (HTTPS). (Cette méthode n'est pas conseillée),

Cette méthode ne peut être utilisée dans le cas d'une authentification externe.

► SRP (Secure Remote Password), utilisation de la méthode sécurisée SRP native, pour le calcul du mot de passe. Avec cette méthode, des champs sont ajoutés dans la fiche LDAP de l'utilisateur avec son login, mot de passe,

► SRP (hash LDAP), utilisation particulière de la méthode SRP. Avec cette méthode, plus besoin de champs login, mot de passe stockés dans la fiche LDAP. Ce sont les logins, mots de passe utilisateur de la base LDAP qui sont utilisés.

Cette méthode est un peu moins sécurisée que le SRP natif (lors d'un accès à la base LDAP, le mot de passe du SRP natif est plus résistant à la méthode de force brute que le mot de passe du SRP Hash. Par contre, les échanges réseau sont tout aussi sécurisés pour les deux méthodes) mais elle permet de réutiliser le mot de passe LDAP classique (champ userpassword).

Méthodes sans mot de passe LDAP

► Certificat (SSL) : utilise le certificat de l'utilisateur stocké dans la base LDAP et installé sur le poste client,

► RADIUS : utilise une authentification via un serveur RADIUS (Voir Chapitre VI « Configuration de l'authentification »),

► Kerberos : utilise une authentification via un serveur Kerberos (Voir Chapitre VI « Configuration de l'authentification »),

► NTLM : utilise une authentification via un serveur NTLM (Voir Chapitre VI « Configuration de l'authentification »).

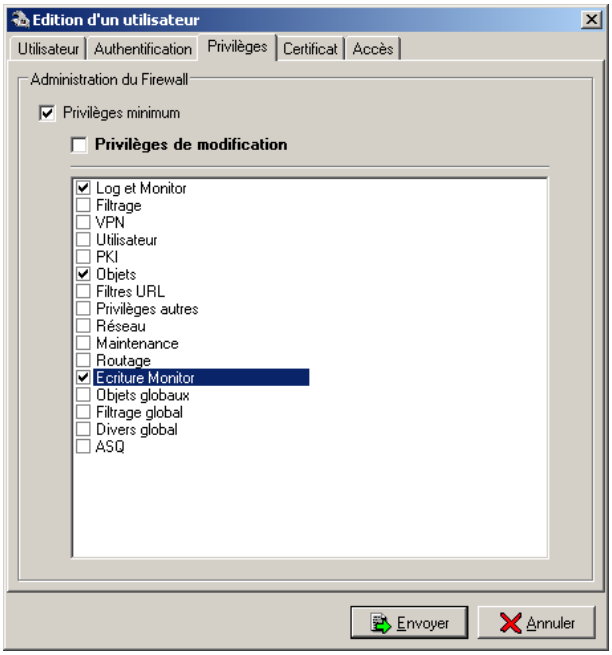
Modifier le mot de passe de l'utilisateur en cliquant sur le bouton « Modifier le mot de passe de l'utilisateur ». Ce mot de passe sera utilisé pour l'authentification au travers du firewall et si l'utilisateur désire se connecter au firewall pour lire ou modifier la configuration. Le champ

« Méthode de hash » vous permet changer la méthode de hachage appliquée au mot de passe (voir section Configuration de l'authentification). L'option « Pas de changement » vous permet de conserver la méthode déjà utilisée.

Calendrier

Cette option permet de spécifier les périodes d'authentification permises pour l'utilisateur. Dans ce calendrier, lorsque l'authentification n'est pas permise, il est impossible pour l'utilisateur de s'authentifier. (Voir « Configuration des calendriers »).

Onglet Privilèges



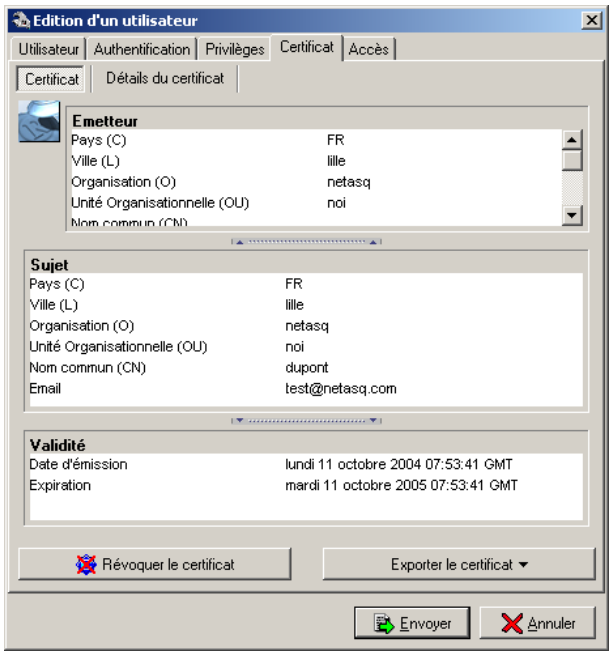
Cette section vous permet de définir les droits de lecture et de modification de la configuration du firewall.

Liste des droits :

► Privilèges minimum, nécessaire pour un utilisateur désirant se connecter à un IPS-Firewall,
► Privilèges de modification, permet d'avoir le droit de modifier la configuration de l'IPS-Firewall,
► **Log et monitor** : droit de consultation des traces,
► **Filtrage** : droit de consultation des règles de filtrage,
► **VPN** : droit de consultation des configurations VPN,
► **Utilisateurs** : droit de consultation des informations sur les utilisateurs,
► **PKI** : droit de consultation des informations de la PKI,
► **Objets** : droit de consultation des objets,
► **Filtres URL** : droit de consultation du filtrage d'URL,
► **Réseau** : droit d'édition de la configuration réseau (interfaces, bridges, dialups, VLANs et configuration dynamique du DNS),
► **Maintenance** : droit permettant les opérations de maintenance (sauvegarde, restauration, mise à jour, arrêt et redémarrage de l'IPS-Firewall, modification de la fréquence de mise à jour de l'antivirus et mise à jour de l'antivirus et enfin les actions liées au RAID dans le moniteur),
► **Routage** : droit d'édition du routage sur les IPS-Firewalls (route par défaut, routes statiques et réseaux de confiance),
► **Ecriture Monitor** : droit permettant d'effectuer certaines opérations nécessitant des droits de modification sans pour autant Bloquer les privilèges de modification « généraux »,
► **Objets globaux, Filtrage global, divers global** : droits permettant d'accéder à la configuration globale,
► **ASQ** : droit de consultation de la configuration de l'ASQ.

© Copyright NETASQ 2006

Onglet certificat



Génération d'un certificat

Cet onglet vous permet de gérer le certificat x509 de l'utilisateur.

Ce certificat peut servir dans deux cas : authentification via SSL et accès en VPN à l'IPS-Firewall avec un client mobile IPSEC. Ce certificat peut aussi être utilisé par d'autres applications.

Pour créer un certificat, (vous devez avoir, au préalable, configuré la PKI interne Voir Chapitre VI « Configuration de l'authentification ») reportez-vous à la procédure suivante :

1. Cliquez sur le bouton « Créer le certificat de l'utilisateur »,

2. Saisissez le mot de passe que vous avez affecté à l'autorité de certification (CA) de l'IPS-Firewall,

3. Indiquez ensuite le mot de passe choisi pour le conteneur PKCS#12 de l'utilisateur. Ce conteneur pourra être exporté sur la machine de l'utilisateur.

Une fois le certificat de l'utilisateur généré, le contenu de celui-ci s'affiche. Vous pouvez alors visualiser tous les champs du certificat (Informations relatives à l'autorité de certification intégrée à l'IPS-Firewall NETASQ, informations relatives à l'utilisateur et période de validité du certificat).

En cliquant sur « Détails des certificats », vous pourrez visualiser le contenu brut du certificat.

Révocation d'un certificat

Le certificat d'un utilisateur peut être révoqué (annulé). Dans ce cas, l'utilisateur ne pourra plus s'authentifier sur le firewall (si la méthode d'authentification choisie est SSL), ni réaliser de VPN (si la méthode d'authentification est basée sur les certificats). Il ne pourra plus utiliser les applications intégrées dans la PKI (utilisant les certificats x509 de la PKI du firewall).

Attention, pour que la révocation prenne effet, il faut regénérer la CRL (Certificate Revocation List). (voir Chapitre VI « Configuration de l'authentification »). Si vous avez d'autres applications qui utilisent les certificats de la PKI du firewall, il faudra alors leur distribuer cette CRL. Les certificats générés par la PKI contiennent un lien vers cette CRL.

Exporter le certificat

Vous pouvez enregistrer le certificat généré. Ainsi vous pouvez l'installer sur le poste utilisateur.

Le certificat peut être exporté au format PKCS#12 (recommandé) ou au format .der. Le conteneur PKCS#12 contient la clé privée et le certificat alors que le format .der ne contient que le certificat.

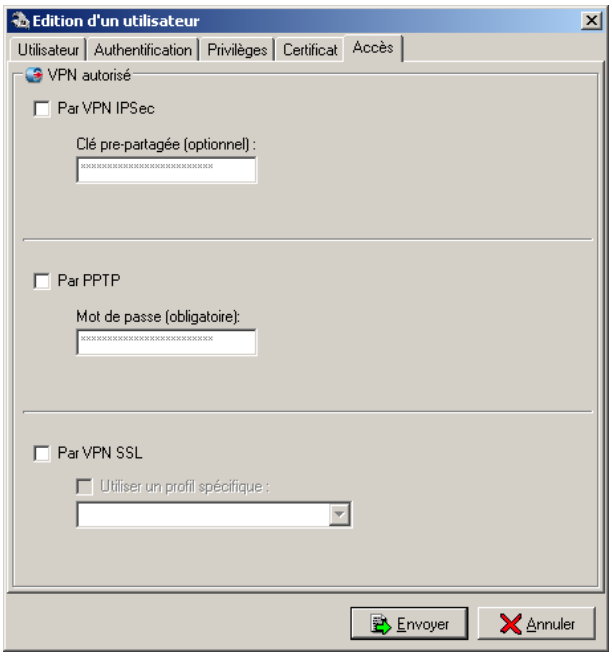
Installation d'un certificat sous Windows

1. Copier le certificat ou le conteneur PKCS#12 en local, sur la machine utilisateur,

2. Ouvrez le fichier. L'installation du certificat débute,

3. Le mot de passe du conteneur PKCS#12 défini lors de la création du certificat est demandé pour terminer l'installation du certificat. Le certificat est alors ajouté aux certificats déjà installés sur le poste utilisateur.

Accès VPN



Cette section vous permet de définir les accès VPN IPSEC et PPTP.

Clef pré-partagée pour IPSEC.

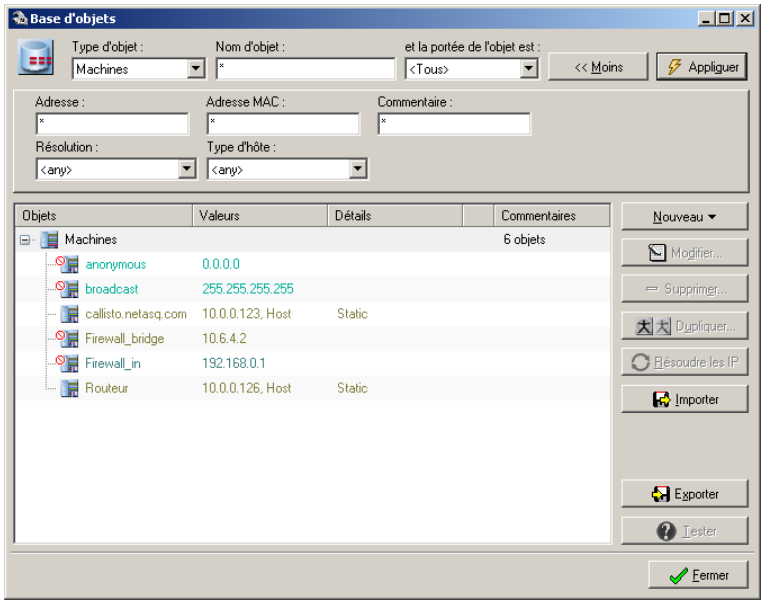
Cette clé sera utilisée pour la création d'un tunnel IPSEC dynamique avec un client mobile IPSEC. Cette même clé devra être indiquée au niveau de la configuration du client mobile de l'utilisateur. (De même, au niveau du client mobile, l'identifiant devra être l'adresse mail de l'utilisateur, définie dans la fiche de l'utilisateur interne au firewall). Ce champ est optionnel, il n'est utilisé que dans le cas d'un tunnel en pre-shared key. Dans le cas contraire, on utilise le certificat de l'utilisateur (plus besoin alors de saisir la clé pre-partagée). Dans tous les cas, le tunnel VPN doit être configuré (au niveau du firewall et du client mobile) en mode agressif, avec un identifiant de type user@fqdn (qui sera l'adresse e-mail de l'utilisateur pour le correspondant). (Voir « Configuration du VPN IPSEC »).

Mot de passe pour PPTP.

Le mot de passe indiqué ici pourra être utilisé par l'utilisateur lorsqu'il voudra se connecter à l'IPS-Firewall en PPTP. (Voir « Configuration du VPN PPTP »).

VPN SSL

Sélectionnez l'option VPN SSL pour permettre à l'utilisateur de bénéficier des fonctionnalités de VPN SSL. (Voir « Configuration du VPN SSL »). Un profil d'utilisation spécifique à cet utilisateur peut être appliqué s'il a été défini dans la configuration du module VPN SSL.



Ce menu vous permet de configurer le nom des machines utilisées dans vos fichiers de configuration. Cette dénomination permet au IPS-Firewall NETASQ de connaître la correspondance entre un nom de machine et son adresse IP.

Chaque entrée de la liste est composée des éléments suivants :

Nom	Nom que vous associez à l'adresse IP.
Type de résolution	Choisir parmi « Statique », « Semi-dynamique » ou « Dynamique » le type de résolution prévue pour cet objet. En sélectionnant « Statique », l'adresse saisie n'est jamais modifiée. En sélectionnant « Semi-dynamique », l'adresse pour ces objets est trouvée à l'aide d'une résolution DNS effectuée manuellement depuis le manager. En sélectionnant « Dynamique », la résolution DNS est faite par l'IPS-Firewall de manière périodique (toutes les 5 minutes). Les fonctionnalités utilisant ces objets ne gèrent pas l'actualisation des données (réactivation manuelle du slot de filtrage nécessaire pour prendre en compte les modifications des objets).
IP	Adresse IP de la machine.
Adresse MAC	Adresse MAC de la machine. Spécifier cette valeur vous permet d'associer une adresse MAC et une adresse IP afin d'éviter l'usurpation de la machine.
Type de l'hôte	Champ de type informationnel vous permettant d'effectuer un niveau de recherche supplémentaire. Vous pouvez choisir parmi : « Hôte », « Serveur » ou « Routeur ».
Commentaire	Commentaires que vous voulez associer à cet objet.

Cliquez sur le bouton « Modifier » pour modifier l'objet. Si vous possédez des slots de filtrage, de filtrage d'URL, de VPN ou de translation d'adresses associés à cet objet, une fenêtre d'information vous demande si vous voulez réactiver ces slots et prendre en compte immédiatement cette

© Copyright NETASQ 2006

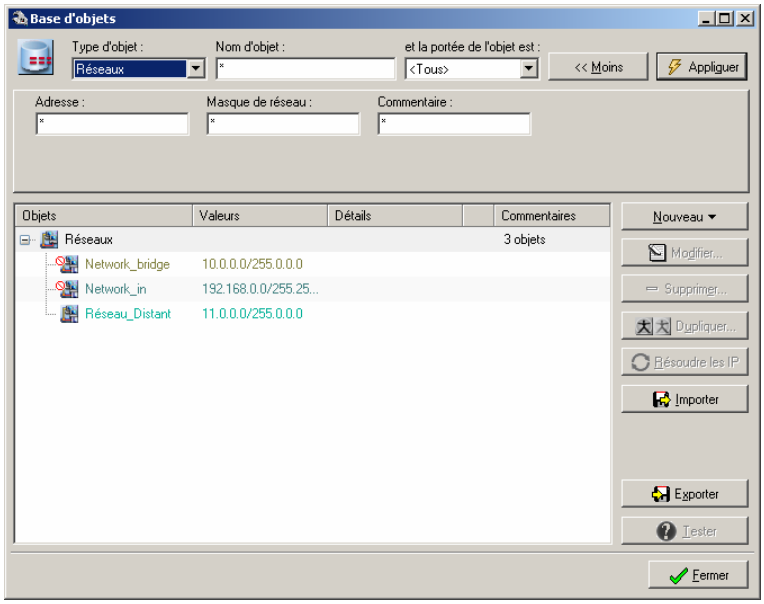
modification. Les slots pour lesquels l'objet est utilisé sont cochés, par défaut, mais vous pouvez désélectionner un type de slot afin de ne pas le réactiver.

Attention, le slot VPN n'est jamais coché même si l'objet est utilisé. Il faudra donc le sélectionner manuellement. Ensuite, la réactivation d'un slot de NAT entraîne la perte des connexions actives.

La résolution dynamique DNS des objets NETASQ n'a pas été conçue pour la modification des politiques de sécurité présentes sur les IPS-Firewalls. En effet étant donné que cette résolution dépend d'un équipement externe à l'IPS-Firewall, celui-ci ne peut en aucun cas valider dynamiquement les modifications de la politique de sécurité. Le contournement de ce mécanisme doit être réalisé par l'administrateur (duplication de la politique de sécurité et activation alternée de deux slots par exemple) avec les incidences que cela entraîne (activation d'une politique de sécurité compromise).

La suppression d'un nom d'objet entraîne l'affichage d'une boîte de dialogue vous invitant à confirmer la suppression et à retirer cette machine des différents groupes de machines où elle était présente.

Il existe des machines pré-configurées : « Firewall_in », « Firewall_out », « Firewall_dmz », « Firewall_bridge », « Firewall_vlan » correspondent aux adresses IP de l'interface interne, externe, DMZ, pont et vlan du Firewall NETASQ. Ces adresses ne sont jamais modifiables dans la partie configuration des objets



Ce menu vous permet de configurer le nom des réseaux et sous-réseaux utilisés dans vos fichiers de configuration. Cette dénomination permet à l'IPS-Firewall NETASQ de connaître la correspondance entre un nom de réseau, son adresse IP et son masque de réseau.

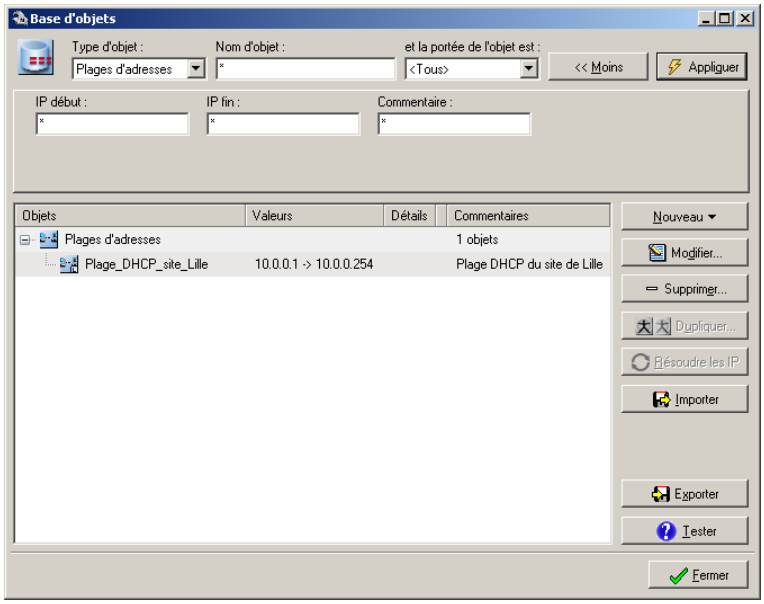
Chaque entrée de la liste est composée d'un nom de réseau, de l'adresse IP de ce réseau, de son masque de réseau et des commentaires sur ce réseau.

Cliquez sur le bouton « Modifier » pour modifier l'objet. Si vous possédez des slots de filtrage, de filtrage d'URL, de VPN ou de translation d'adresses associés à cet objet, une fenêtre d'information vous demande si vous voulez réactiver ces slots et prendre en compte immédiatement cette modification. Les slots pour lesquels l'objet est utilisé sont cochés, par défaut, mais vous pouvez désélectionner un type de slot afin de ne pas le réactiver. Attention, le slot VPN n'est jamais coché même si l'objet est utilisé. Il faudra donc le sélectionner manuellement. Ensuite, la réactivation d'un slot de NAT entraîne la perte des connexions actives.

La suppression d'un réseau entraîne l'affichage d'une boîte de dialogue vous invitant à confirmer l'action et à retirer ce réseau des différents groupes de réseau où il était présent.

Il existe des réseaux pré-configurés : « Network_in », « Network_out » et « Network_dmz » correspondent aux réseaux interne, externe et à la DMZ. Si vous utilisez l'IPS-Firewall en mode transparent seul le « Network_bridge » est crée. Dans le cas où vous avez créé des vlans, les réseaux « Network_vlan » seront créés. Ces noms ne peuvent pas être modifiés.

© Copyright NETASQ 2006

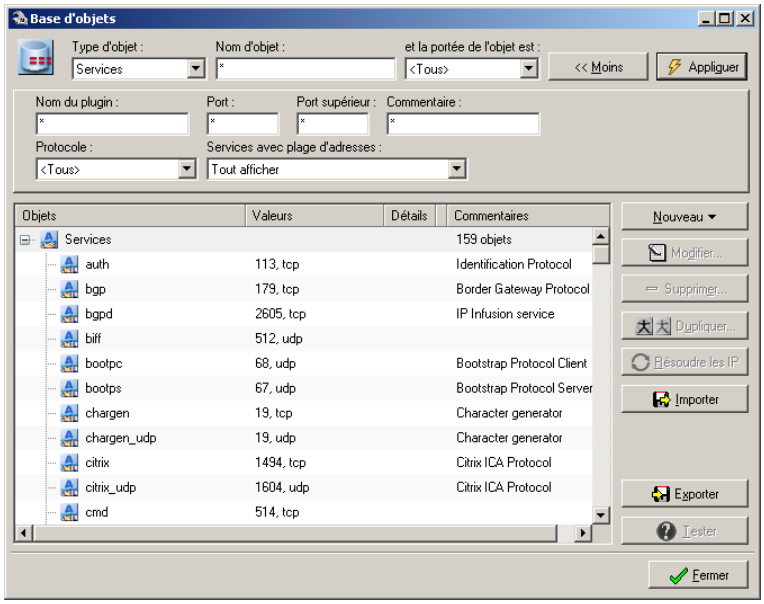


Ce menu vous permet de configurer des plages d’adresses. Ces plages d’adresses pourront être utilisées lorsqu’il s’agit de spécifier un pool d’adresses particulières (DHCP, PPTP, etc).

Chaque entrée de la liste est composée d’un nom de plage d’adresses, d’une adresse de début, d’une adresse de fin et d’un commentaire.

Cliquez sur le bouton « Modifier » pour modifier l’objet. Si vous possédez des slots de filtrage, de filtrage d'URL, de VPN ou de translation d'adresses associés à cet objet, une fenêtre d'information vous demande si vous voulez réactiver ces slots et prendre en compte immédiatement cette modification. Les slots pour lesquels l'objet est utilisé sont cochés, par défaut, mais vous pouvez désélectionner un type de slot afin de ne pas le réactiver. Attention, le slot VPN n'est jamais coché même si l'objet est utilisé. Il faudra donc le sélectionner manuellement. Ensuite, la réactivation d'un slot de NAT entraîne la perte des connexions actives.

© Copyright NETASQ 2006



Ce menu vous permet de configurer les noms de services utilisés dans vos fichiers de configuration de filtrage. Cette dénomination permet au Firewall NETASQ de connaître la correspondance entre un nom de service, le protocole utilisé et le numéro de port associé.

De plus la colonne « Détails » vous indique quel plugin est associé à quel service. Vous pouvez activer un plugin sur plusieurs services ou activer plusieurs plugins sur un seul service. De plus un plugin n'est pas réservé à un type de service. Par exemple le plugin HTTP n'est pas réservé au trafic HTTP. Vous pouvez forcer l'activation du plugin pour d'autres types de services. Cela vous permet d'associer un plugin à un port généralement utilisé pour un trafic défini mais que vous utilisez pour un autre type de trafic.

Lorsque vous avez spécifié un plugin pour un service ce plugin ne s'active que lorsque le service est utilisé dans une règle de filtrage.

Pour une activation automatique du plugin, même si aucune règle directement associée au service n'a été spécifiée reportez vous à la section « Configuration de l'ASQ – plugins ».

Attention, pour un maximum de sécurité, NETASQ vous recommande l'utilisation forcée du plugin plutôt qu'une activation automatique. L'activation automatique des plugins doit être réservée à la réalisation de services non critiques pour votre sécurité (la création de logs visant à réaliser un monitoring du trafic HTTP par exemple).

Chaque entrée de la liste est composée d'un nom de service, du nom de protocole, du numéro de port associé au service (ou d'une plage de ports encadrée par les champs « Port du service » et « Inclure les ports jusqu'au »), des commentaires sur ce service ainsi que le plugins associé à ce service. Les services TCP et UDP sont mélangés dans cette liste.

Cliquez sur le bouton « Modifier » pour modifier l'objet. Si vous possédez des règles de filtrage associées à cet objet, une fenêtre d'information vous demande si vous voulez réactiver ces règles de filtrage et prendre en compte immédiatement cette modification.

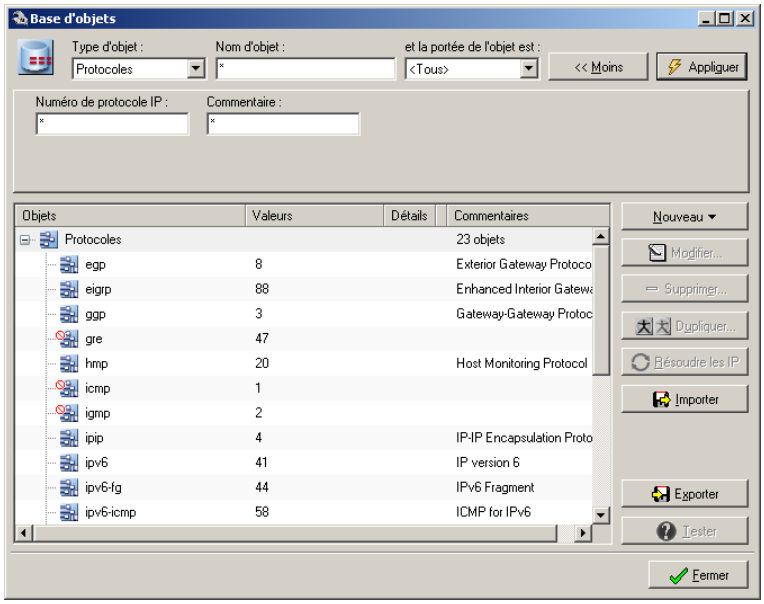
Cette version de l'IPS-Firewall NETASQ ne gère pas les services RPC (Remote Procedure Call), lesquels utilisent un numéro de port alloué dynamiquement.

© Copyright NETASQ 2006

Certains services ne sont pas modifiables. Par ailleurs, il existe un service réservé pour le fonctionnement de l'IPS-Firewall :

« Firewall_srv » (port 1300) correspond à un nom de service qui gère la communication entre le Firewall NETASQ et le Firewall Manager, Firewall Monitor. Ce service est aussi utilisé pour les échanges nécessaires à la fonctionnalité de haute disponibilité entre deux firewalls.

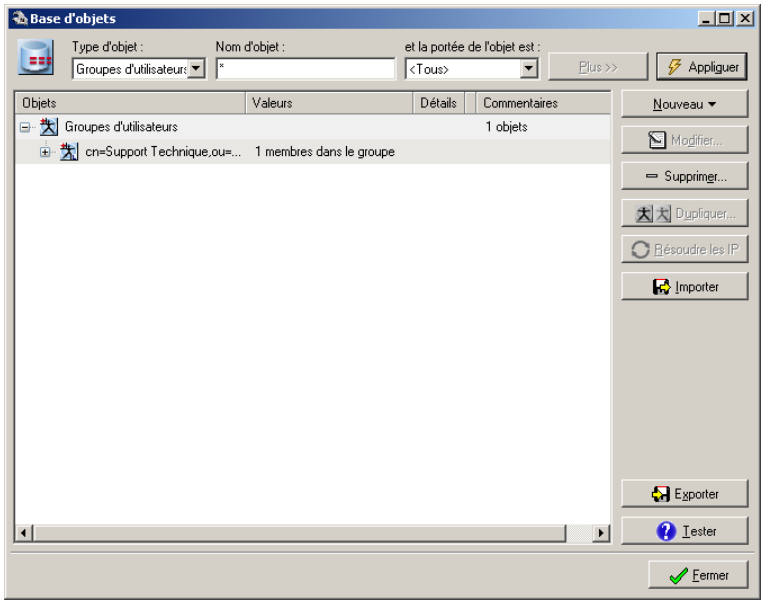
Vous trouverez en Annexe B une liste de services souvent utilisés (DNS, HTTP, FTP...), ainsi que le protocole et le numéro de port associés à ce service.



Ce menu vous permet de configurer les noms de protocoles fonctionnant sur IP utilisés dans la configuration du filtrage. Cela renseigne le firewall sur la correspondance entre un nom et le numéro de protocole utilisé par la couche IP. Tout protocole supporté par IP peut être ajouté et géré par le Firewall.

Cela vous permet ensuite d'utiliser ces noms dans les règles de filtrage et d'appliquer une politique de sécurité pour ces protocoles.

© Copyright NETASQ 2006



Ce menu vous permet de créer des groupes d'utilisateurs. Ces groupes simplifient l'édition des règles de filtrage : au lieu de définir une règle pour chaque utilisateur, vous définissez une règle pour tous les utilisateurs ayant les mêmes droits.

Pour créer un nouveau groupe, reportez-vous à la procédure suivante :

1. Cliquez sur le bouton « Ajouter », un assistant de création apparaît,

2. Saisissez tout d'abord, le nom que vous voulez donner au groupe, puis, éventuellement, une description du groupe,

3. Vous pouvez alors choisir le premier utilisateur du groupe dans la grille proposée. Puis cliquez sur « Terminer ».

Ajouter un utilisateur dans un groupe

Pour ajouter un utilisateur dans un groupe d'utilisateur, suivez la procédure suivante :

1. Sélectionnez l'utilisateur que vous désirez ajouter dans la grille de définition des objets,

2. Cliquez sur le bouton droit de votre souris,

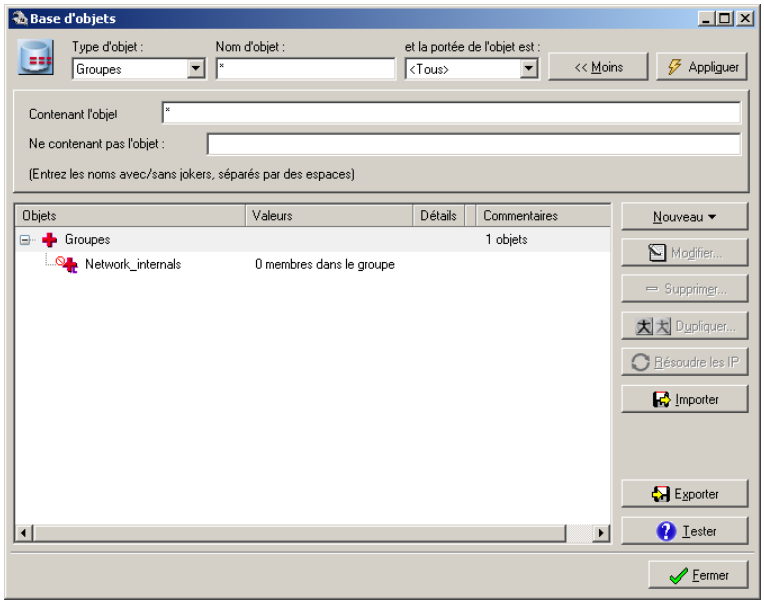
3. Sélectionnez l'option « Ajouter à » dans le menu contextuel apparu,

4. Choisissez le groupe dans lequel doit être ajouté l'utilisateur.

Si vous ajoutez un utilisateur dans un nouveau groupe, l'utilisateur est automatiquement spécifié dans la fenêtre de configuration du groupe. Si un groupe utilisé dans la configuration de l'appliance UTM est modifié, cette modification est automatiquement prise en compte par l'appliance UTM et les slots utilisant ce groupe sont automatiquement réactivés.

Attention, la réactivation d'un slot de NAT entraîne la perte des connexions actives.

© Copyright NETASQ 2006



Ce menu vous permet de créer ce qu'on appellera des groupes « réseau ». Ces groupes pourront contenir des Machines, des réseaux, des plages d'adresses ou encore d'autres groupes « réseau ».

Ajouter un objet dans un groupe « réseau »

Pour ajouter un objet dans un groupe « réseau », suivez la procédure suivante :

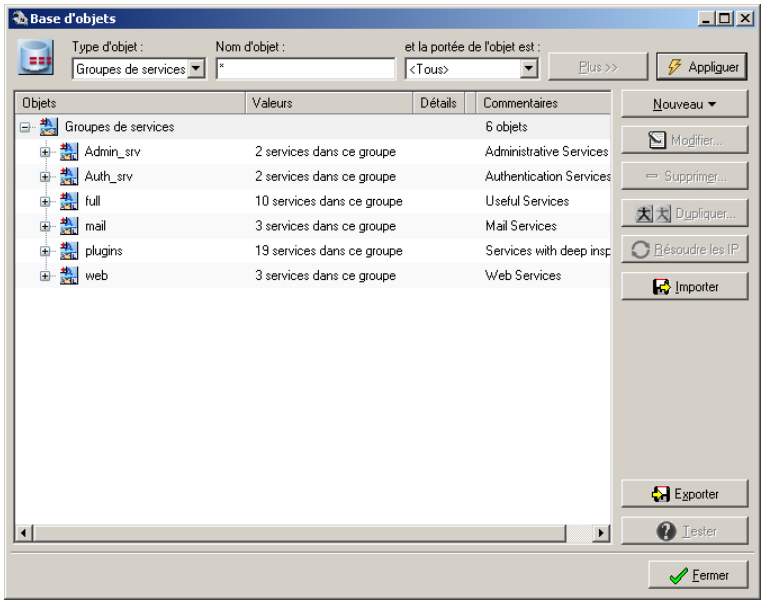
1. Sélectionnez l'objet que vous désirez ajouter dans la grille de définition des objets,
2. Cliquez sur le bouton droit de votre souris,
3. Sélectionnez l'option « Ajouter à » dans le menu contextuel apparu,
4. Choisissez le groupe dans lequel doit être ajouté l'objet.

Si vous ajoutez un objet dans un nouveau groupe, le groupe est créé et l'objet est automatiquement ajouté au groupe.

Si un groupe utilisé dans la configuration de l'appliance UTM est modifié, cette modification est automatiquement prise en compte par l'appliance UTM et les slots utilisant ce groupe sont automatiquement réactivés.

Attention, la réactivation d'un slot de NAT entraîne la perte des connexions actives.

© Copyright NETASQ 2006



De même que pour les utilisateurs et les équipements réseaux, vous pouvez constituer des groupes de services avec des services qui possèdent les mêmes propriétés de configuration. Ces groupes de services pourront ensuite être utilisés dans la configuration comme un seul et même service.

Ceci a pour but de simplifier la configuration et la compréhension de votre configuration en limitant le nombre de services à intégrer.

Ajouter un service dans un groupe

Pour ajouter un service dans un groupe, suivez la procédure suivante :

1. Sélectionnez le service que vous désirez ajouter dans la grille de définition des objets,
2. Cliquez sur le bouton droit de votre souris,
3. Sélectionnez l'option « Ajouter à » dans le menu contextuel apparu,
4. Choisissez le groupe dans lequel doit être ajouté le service.

Si vous ajoutez un service dans un nouveau groupe, le service est automatiquement ajouté au groupe.

Si un groupe utilisé dans la configuration de l'appliance UTM est modifié, cette modification est automatiquement prise en compte par l'appliance UTM et les slots utilisant ce groupe sont automatiquement réactivés.

Attention, la réactivation d'un slot de NAT entraîne la perte des connexions actives.

Le Firewall contient quelques groupes de service pré-configurés qui permettent de faciliter la configuration :

© Copyright NETASQ 2006

Full	Contient les services qui permettent un accès au web, mail, telnet et les principaux services autour du web (news, ftp, DNS ...).
Mail	Contient tous les services d'accès au mail pour les clients.
Web	Services uniquement d'accès web (http et https).
Plugins	Services possédant un plugin spécifique et les plugin associés activés.
Admin_srv	Services d'administration de l'IPS-Firewall (SSH et firewall_srv).
Auth_srv	Services d'authentification sur l'IPS-Firewall (HTTPS et firewall_auth).

Il existe des noms d'objets réservés :

► De manière générale tous les noms d'objets commençant par « firewall_ » et « network_ » sont interdits,

► Les noms de protocoles TCP, UDP, ICMP, IGMP, ESP, AH et GRE sont réservés,

► Dans le cas des services, ssh, isakmp, firewall_srv, firewall_auth, ephemeral_tcp, ephemeral_udp et ephemeral_fw.

Ces noms d'objets réservés sont signalés dans les différentes listes d'objets par un panneau à côté du nom d'objet. Ces noms ne peuvent jamais être modifiés.

© Copyright NETASQ 2006

Section C

Prévention d’intrusion (ASQ)

Pour cette section, vous devez avoir franchi les étapes

► Installation, pré-configuration, intégration.

Pour cette section, vous devez connaître

► Les actions à engager lors de la détection d'attaques,
► Les informations relatives à la configuration du stateful,
► Les ports que vous voulez surveiller,
► Les protocoles applicatifs que vous voulez analyser.

Utilité de la section

Cette section vous permet de configurer le noyau ASQ, cœur d'un IPS-firewall NETASQ, notamment les actions à effectuer lorsque des attaques sont détectées. De plus la configuration du stateful, du routage, des sondes et des plug-ins complète la configuration de l'IPS-Firewall avant la mise en place de politiques de filtrage, de translations, etc.

Les fonctions d'alarme du noyau ASQ permettent, suite à l'enregistrement d'un événement de sécurité possédant un niveau d'alarme, d'effectuer les actions suivantes :

► Allumer le voyant correspondant au niveau de l'alarme sur la face avant du boîtier appliance IPS-Firewall/VPN,
► Afficher l'alarme sur le Firewall Monitor,
► Envoyer l'alarme par email aux utilisateurs spécifiés.

Accéder à cette section

Accédez à la boîte de dialogue par le menu « Prévention d'intrusion » de l'arborescence des menus du Firewall Manager.

Vous devez être connecté avec les privilèges de modification pour pouvoir effectuer ces modifications.

Avant d'effectuer toute modification importante sur votre NETASQ Firewall, nous vous conseillons d'effectuer une sauvegarde. Ainsi, en cas de mauvaise manipulation vous pourrez vous revenir dans la configuration précédente.

© Copyright NETASQ 2006

L'ASQ, moteur de détection et de prévention d'intrusion, est intégré dans toute la gamme des boîtiers IPS-firewalls NETASQ. Anticipant dès sa création l'évolution des technologies de sécurité Internet, les laboratoires de Recherche et Développement de NETASQ ont mis au point l'ASQ dès 1998. Ce moteur intelligent intègre un système de prévention d'intrusion (IPS : Intrusion Prevention System) qui détecte et élimine tout comportement malicieux en temps réel.

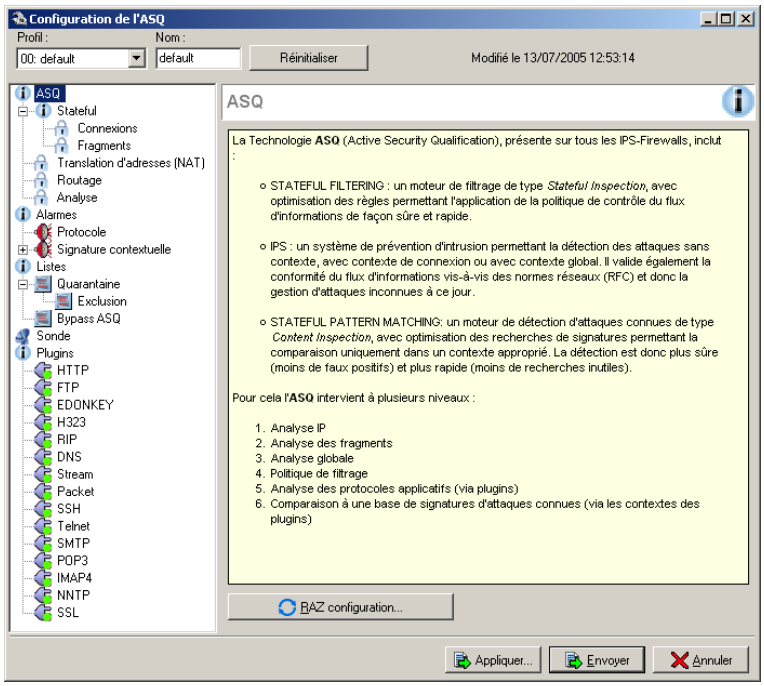
De nos jours, les contre-mesures sont très compliquées à mettre en place et très ciblées vis-à-vis des d'attaques de type « déni de service » par exemple. En effet, d'un point de vue théorique, la plupart des attaques visant à créer des dénis de service sont basées sur des services ou protocoles standard sur Internet. S'en protéger reviendrait à couper les voies de communications normales avec Internet, alors que c'est la raison principale des machines concernées (serveurs web, de messagerie, etc...).

Pourtant, il faut tout de même agir pour garantir la sécurité des données de l'entreprise. Tout cela implique beaucoup de démarches : il faut monitorer le trafic (ce qui est loin d'être simple, du fait de la quantité de données qui transitent), établir des profils types de comportement et des écarts tolérables au-delà desquels on considérera que l'on fait l'objet d'une attaque; il faut également définir les types d'attaques contre lesquelles on souhaite se protéger (analyses de risques à l'appui) car il est impossible de toutes les prévoir. Il s'agit de mettre en place une protection intelligente et flexible.

L'ASQ répond à ces contraintes et, grâce à son analyse du trafic, prévient les grandes familles d'attaques en temps réel.

Le menu de configuration de l'ASQ est divisé en deux parties :

► A gauche un arbre présentant les diverses fonctionnalités du menu ASQ,
► A droite les options configurables.


Configuration de l'ASQ
Profil :
00: default
Nom :
default
Réinitialiser
Modifié le 13/07/2005 12:53:14
ASQ
Stateful
Connexions
Fragments
Translation d'adresses (NAT)
Routage
Analyse
Alarmes
Protocole
Signature contextuelle
Listes
Quarantaine
Exclusion
Bypass ASQ
Sonde
Plugins
HTTP
FTP
EDONKEY
H323
RIP
DNS
Stream
Packet
SSH
Telnet
SMTP
POP3
IMAP4
NNTP
SSL
ASQ
La Technologie ASQ (Active Security Qualification), présente sur tous les IPS-Firewalls, inclut :
STATEFUL FILTERING : un moteur de filtrage de type Stateful Inspection, avec optimisation des règles permettant l'application de la politique de contrôle du flux d'informations de façon sûre et rapide.
IPS : un système de prévention d'intrusion permettant la détection des attaques sans contexte, avec contexte de connexion ou avec contexte global. Il valide également la conformité du flux d'informations vis-à-vis des normes réseaux (RFC) et donc la gestion d'attaques inconnues à ce jour.
STATEFUL PATTERN MATCHING: un moteur de détection d'attaques connues de type Content Inspection, avec optimisation des recherches de signatures permettant la comparaison uniquement dans un contexte approprié. La détection est donc plus sûre (moins de faux positifs) et plus rapide (moins de recherches inutiles).
Pour cela l'ASQ intervient à plusieurs niveaux :
1. Analyse IP
2. Analyse des fragments
3. Analyse globale
4. Politique de filtrage
5. Analyse des protocoles applicatifs (via plugins)
6. Comparaison à une base de signatures d'attaques connues (via les contextes des plugins)
RAZ configuration...
Appliquer...
Envoyer
Annuler

Multi profil

Il est désormais possible de créer quatre profils de l'ASQ afin d'adapter l'analyse de l'ASQ en fonction des types de trafic ou du sens du trafic. Cela va permettre de désactiver certaines alarmes sur des trafics autorisés en sortie mais pas en entrée. (Voir « Configuration du filtrage »).

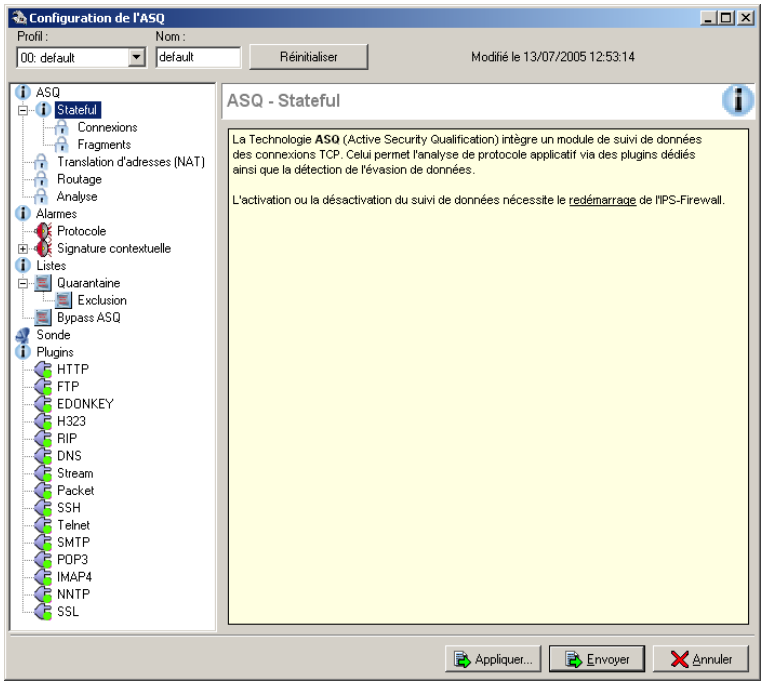
La barre d'action située en haut de l'écran vous indique quel profil de l'ASQ est actuellement affiché. De plus vous pouvez spécifier un nom pour chacun des quatre profils.

Le bouton « Réinitialiser » vous permet de redéfinir les paramètres des profils ASQ dans leur configuration d'origine.

La date située à côté du bouton « Réinitialiser » indique la date de la dernière modification de la configuration.

Application des changements

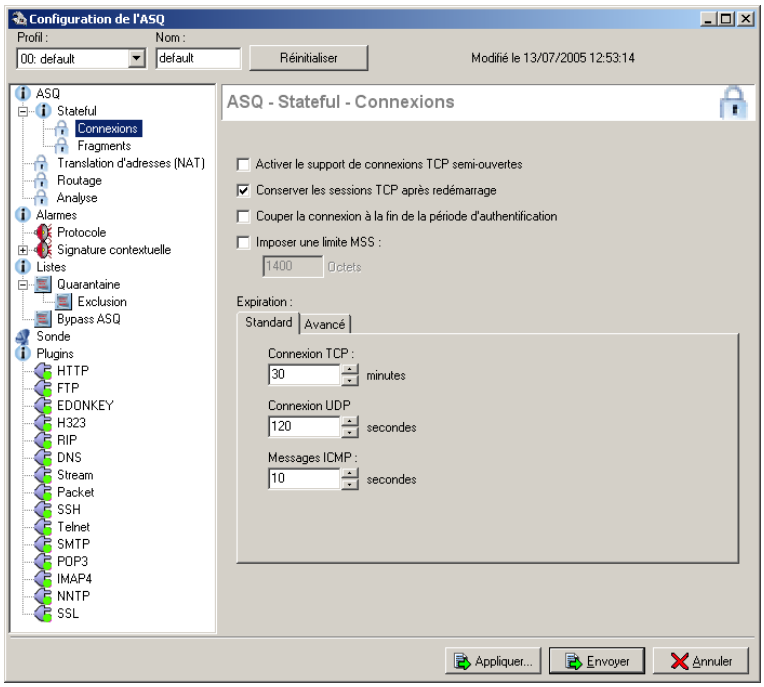
Le bouton « Appliquer » situé dans la barre d'action au bas de la fenêtre de configuration de l'ASQ vous permet d'appliquer les changements configurés sans avoir à envoyer la configuration et donc fermer la fenêtre.



Les paramètres de configuration du module Stateful Inspection, module permettant l'analyse dynamique des paquets, sont modifiables dans l'onglet « Stateful » du menu ASQ de l'arborescence. Ce module, intégré au module ASQ, conserve l'état des connexions et permet l'analyse des paquets pour la détection d'attaques. Le Stateful vous permet de ne définir, dans les règles de filtrage, que les règles aller (règle indiquant le sens de la connexion) sans avoir à préciser la règle retour (réponse de l'hôte contacté par l'émetteur de la connexion).

Le menu de configuration du moteur Stateful est divisé en deux sections : Connexions et Fragments. Les paramètres configurables dans ces sections sont expliqués dans les tableaux suivants.

Connexions



Activer le support de connexions TCP semi-ouvertes	Un des correspondants a clos sa connexion pourtant l'autre continue à émettre des paquets. La connexion est alors unidirectionnelle.
Conserver les sessions TCP après redémarrage	Lorsque cette option est activée, le firewall garde en mémoire le contexte des connexions lorsqu'il redémarre et les connexions ne sont donc pas interrompues. Cette option doit être activée pour que le maintien des connexions soit réalisée lors d'un basculement de firewalls en haute disponibilité.
Couper la connexion à la fin de la période d'authentification	Cette option permet la clôture des connexions actives à la fin de la période d'authentification.
Imposer une limite MSS	L'IPS-Firewall va redimensionner les paquets TCP (et pas UDP) à la taille indiquée dans le champ « Limite MSS ». Cette fonctionnalité est utile pour des connexions de type PPPoE ou VPN car les paquets ne doivent pas dépasser une certaine taille (dans le cas contraire ils sont soit fragmentés, soit rejetés). La valeur conseillée est de 1300 octets.

Attention, l'utilisation de l'option « Activer le support de connexions TCP semi-ouvertes» est déconseillée. En effet la sélection de cette option permet la transmission de paquets plus permissifs pour l'intégrité des ressources protégées par l'IPS-Firewall. Cette option est supportée pour des raisons de compatibilité avec le protocole TCP et n'est à utiliser qu'en connaissance de cause.

Délais d'expiration standards

Des délais d'expiration standards sont configurables sur l'IPS-Firewall. Ils sont expliqués dans le tableau suivant :

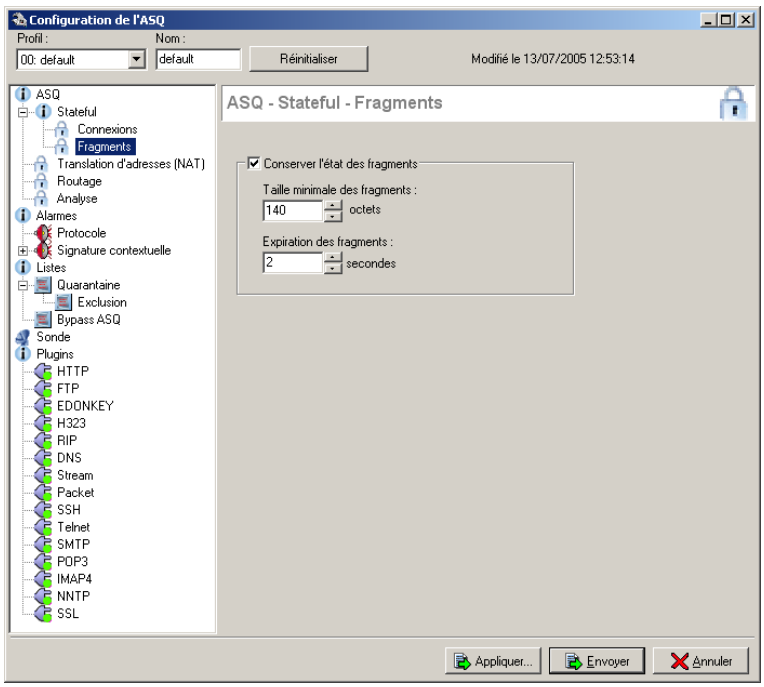
Connexion TCP	Temps au bout duquel les connexions TCP sont réinitialisées.
Connexion UDP	Temps au bout duquel les connexions UDP sont réinitialisées.
Messages ICMP	Temps de conservation des messages ICMP.

Délais d'expiration avancés

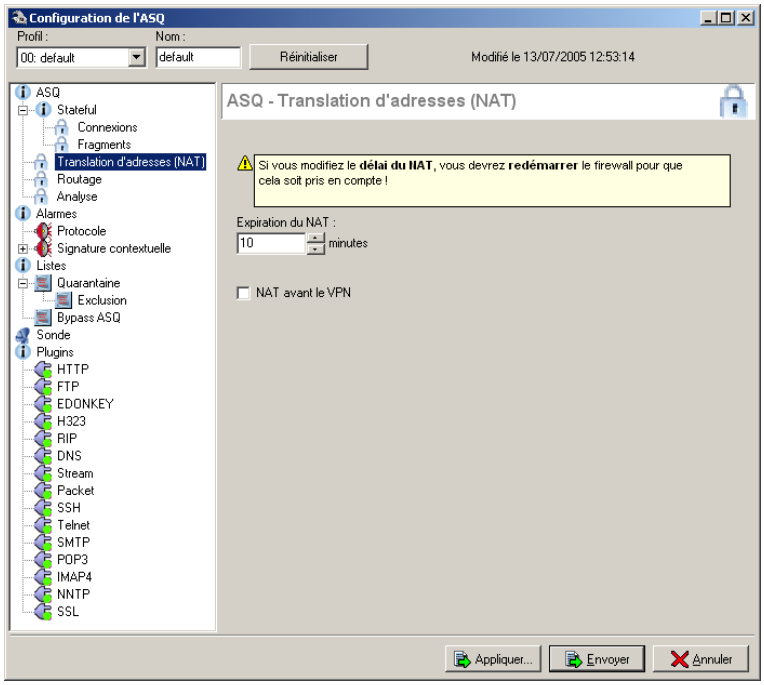
Des délais d'expiration avancés sont configurables sur l'IPS-Firewall. Ils sont expliqués dans le tableau suivant :

Ouverture de connexion	Temps maximum admis pour la phase d'ouverture d'une connexion TCP (SYN, SYN-ACK, ACK).
Fermeture de connexion	Temps maximum admis pour la phase de fermeture d'une connexion TCP (FIN, FIN-ACK, FIN, FIN-ACK).
Connexion fermée	Aucune connexion utilisant les mêmes adresses et ports, sources et destination ne peut débuter durant le délai de « connexion fermée ».
Connexion fille	Temps durant lequel une tentative d'établissement d'une connexion fille est acceptée.
Purge lors de saturation	Lorsque la table des connexions de l'ASQ est pleine et qu'une nouvelle tentative de connexion arrive, l'ASQ tente de supprimer dans sa table, certaines connexions (essentiellement les connexions en établissement) afin de libérer une place. Il ressaie dans l'intervalle défini par cette option.

Fragments



Garder l'état des fragments	Si cette option a été sélectionnée, le firewall analyse les paquets IP fragmentés afin de déterminer les éventuelles attaques de type fragmentation de paquets IP. Si l'option n'est pas sélectionnée, le firewall ne laisse pas passer les paquets fragmentés.
Taille minimale des fragments	Taille minimale d'un fragment. Au minimum 140 octets.
Délai d'expiration des fragments	Temps de conservation des fragments passant par l'IPS-Firewall.

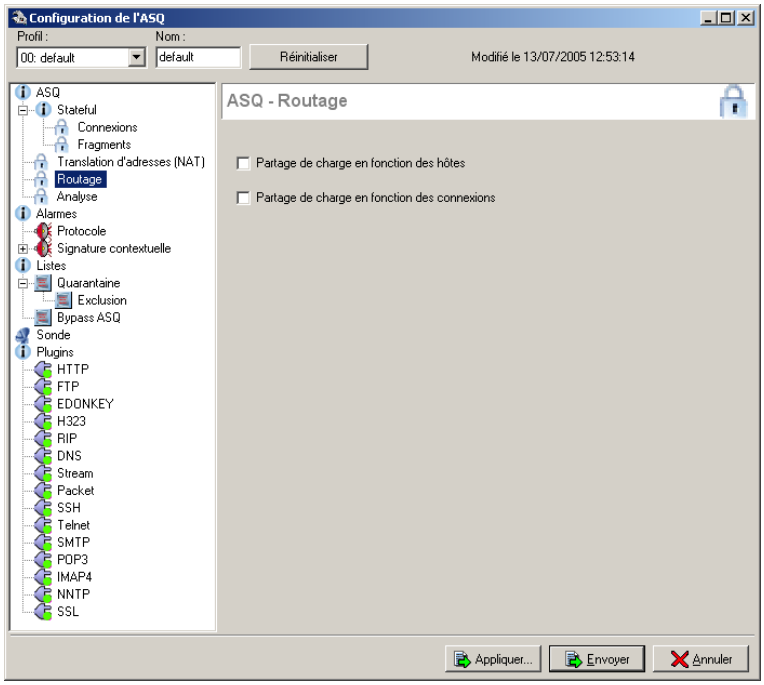


Une section de la configuration de l'ASQ est réservée à l'analyse de la translation d'adresses sur l'IPS-Firewall. Le tableau indique les paramètres configurables.

Délai d'expiration du NAT	Temps au bout duquel les connexions impliquant de la translation d'adresses sont réinitialisées.
NAT avant le VPN	Les fonctionnalités NAT et VPN ont parfois des incompatibilités. En effet le VPN IPSec utilise une fonction de hachage pour authentifier les différents paquets d'une connexion VPN. Cette focntion de hachage est basée sur les informations contenues dans l'entête du paquet. Or les fonctionnalités NAT modifie cet entête. Ainsi l'entête et le hash VPN ne correspondent plus et le paquet associé est rejeté par le correspondant VPN distant. Pour s'affranchir de cette incompatibilité cochez l'option « NAT avant le VPN » afin que les traitements NAT soient pris en compte avant le calcul du hash VPN.

La modification du délai d'expiration des sessions NAT entraîne le redémarrage de l'IPS-Firewall.

© Copyright NETASQ 2006



Les paramètres de configuration du module Routage sont modifiables dans l'onglet « Routage » du menu ASQ de l'arborescence.

Partage de charge en fonction des hôtes et partage de charge en fonction des connexions

Plusieurs mécanismes, intégrés au firewall NETASQ, apportent à votre installation une haute disponibilité d'accès. Ainsi, une liaison spécialisée n'est plus nécessaire pour garder une qualité de service importante et un débit conséquent.

L'option partage de charge de liens des firewalls NETASQ permet d'utiliser deux accès (ou plus) simultanément (de type ADSL, Numéris ou RTC) pour offrir un service de répartition de charge et de haute disponibilité. Le firewall NETASQ redirigera les flux vers l'un ou l'autre des deux accès de façon simultanée. Lorsqu'un des accès devient hors service, le firewall redirige automatiquement tous les flux vers l'accès restant. Il est possible d'utiliser plusieurs accès de même type (exemple : 2 accès ADSL) ou plusieurs accès différents (exemple : 1 accès ADSL + 1 accès RNIS).

De plus, cette fonctionnalité offre la possibilité d'augmenter la bande passante de l'accès Internet. En effet, les bandes passantes des accès sont cumulées.

Configuration

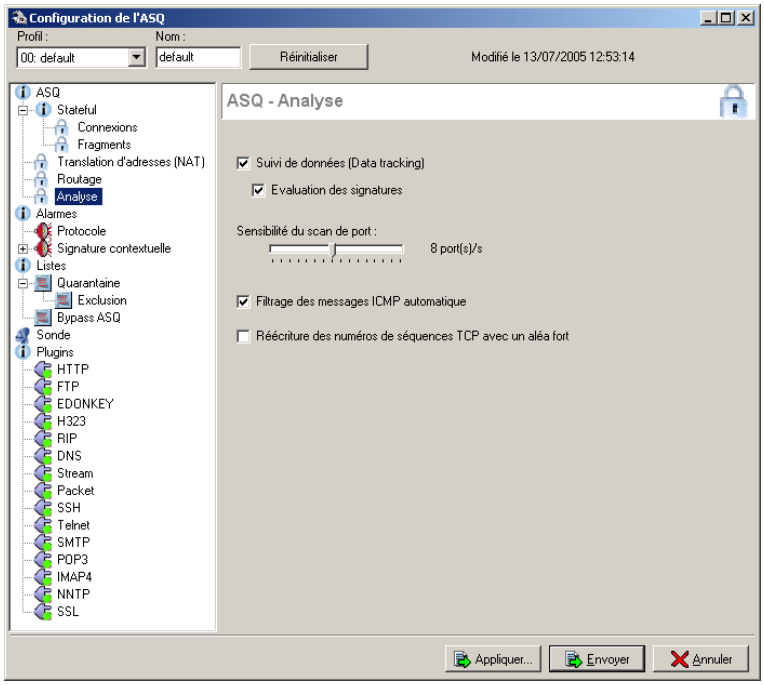
Pour réaliser la configuration du partage, reportez-vous à la procédure suivante :

1. Paramétrez chacun des accès (voir la configuration des Dialup), activez bien l'option « Route par défaut » pour chacun des accès,

2. Sélectionnez ensuite l'option « Partage de charge en fonction des hôtes », puis activez chacun des deux accès. Si vous ne sélectionnez pas cette option, vous ne pourrez pas activer plusieurs accès dialup simultanément.

Lorsque cette option est activée, vous pouvez choisir d'activer le partage de charge de connexion (partage de charge en fonction des connexions). Cette fonctionnalité vous permet de répartir la charge en fonction des connexions (pour chaque connexion, un lien dialup est affecté) alors qu'en fonctionnement normal, la répartition se fait en fonction de la machine source (à chaque adresse IP est affectée un lien dialup).

© Copyright NETASQ 2006



Les paramètres de configuration du module Analyse sont modifiables dans l'onglet « Analyse » du menu ASQ de l'arborescence.

Suivi de données (Data Tracking)

L'IPS-Firewall analyse la cohérence entre les données contenues dans le paquet et son entête ainsi que la cohérence entre plusieurs paquets fragmentés (pour éviter l'évasion de données).

L'activation ou la désactivation du Suivi de données (Data Tracking) entraîne le redémarrage de l'IPS-Firewall.

Evaluation des signatures

Cette option permet l'activation des analyses basées sur les signatures contextuelles.

Détection de scan de ports

Si cette option est sélectionnée, l'IPS-Firewall peut détecter les scans de ports y compris les scans furtifs (scans se basant sur les réponses des machines aux paquets FIN et pas aux paquets SYN. Ces scans sont, dans la majorité des cas, non tracés au niveau des machines scannées puisqu'aucun paquet SYN n'a été reçu). Il est possible de déterminer le nombre de ports pouvant être scannés avant le déclenchement de l'alarme.

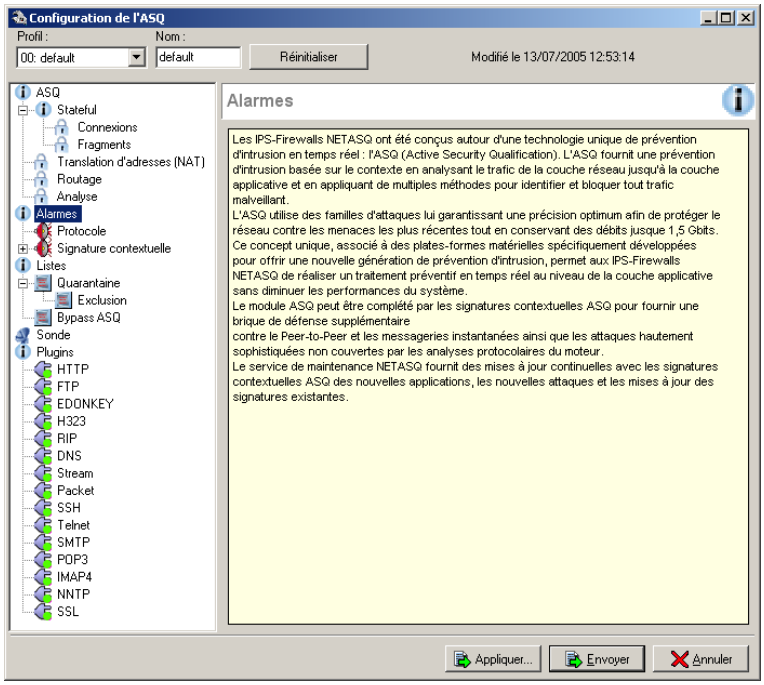
Filtrage des messages ICMP automatique

Cette option permet d'autoriser le passage de messages ICMP si ceux-ci sont cohérents dans une connexion TCP, UDP ou ICMP (filtrage intelligent des paquets ICMP).

Réécriture des numéros de séquences TCP avec un aléa fort

Afin de pallier aux systèmes générant des paquets avec des numéros de séquence peu aléatoires, il est possible d'activer cette option. L'IPS-Firewall va « réécrire » les paquets avec un numéro de séquence beaucoup plus imprédictible.

© Copyright NETASQ 2006


Configuration de l'ASQ
Profil :
00: default
Nom :
default
Réinitialiser
Modifié le 13/07/2005 12:53:14
ASQ
Stateful
Connexions
Fragments
Translation d'adresses (NAT)
Routage
Analyse
Alarmes
Protocole
Signature contextuelle
Listes
Quarantaine
Exclusion
Bypass ASQ
Sonde
Plugins
HTTP
FTP
EDONKEY
H323
RIP
DNS
Stream
Packet
SSH
Telnet
SMTP
POP3
IMAP4
NNTP
SSL
Alarmes
Les IPS-Firewalls NETASQ ont été conçus autour d'une technologie unique de prévention d'intrusion en temps réel : l'ASQ (Active Security Qualification). L'ASQ fournit une prévention d'intrusion basée sur le contexte en analysant le trafic de la couche réseau jusqu'à la couche applicative et en appliquant de multiples méthodes pour identifier et bloquer tout trafic malveillant.
L'ASQ utilise des familles d'attaques lui garantissant une précision optimum afin de protéger le réseau contre les menaces les plus récentes tout en conservant des débits jusque 1,5 Gbits.
Ce concept unique, associé à des plates-formes matérielles spécifiquement développées pour offrir une nouvelle génération de prévention d'intrusion, permet aux IPS-Firewalls NETASQ de réaliser un traitement préventif en temps réel au niveau de la couche applicative sans diminuer les performances du système.
Le module ASQ peut être complété par les signatures contextuelles ASQ pour fournir une brique de défense supplémentaire
contre le Peer-to-Peer et les messageries instantanées ainsi que les attaques hautement sophistiquées non couvertes par les analyses protocolaires du moteur.
Le service de maintenance NETASQ fournit des mises à jour continuelles avec les signatures contextuelles ASQ des nouvelles applications, les nouvelles attaques et les mises à jour des signatures existantes.
Appliquer...
Envoyer
Annuler

Pour chacune des attaques gérées par les IPS-Firewalls NETASQ, l'administrateur possédant les droits « *+M » peut définir si les paquets incriminés doivent être transmis ou détruits et s'il y a lieu de générer un événement de sécurité possédant un niveau d'alarme, automatiquement enregistré dans le fichier de trace « alarmes ».

La liste présentée dans cette fenêtre regroupe toutes les attaques et familles d'attaques gérées par les IPS-Firewalls.

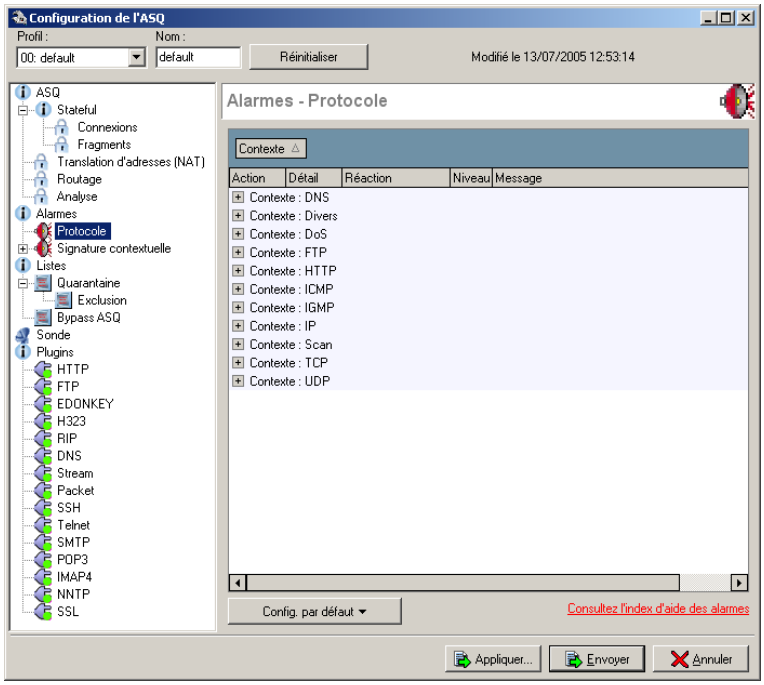
Les alarmes sont divisées en deux catégories :

► Les alarmes de catégorie « Protocole » : associées aux analyses protocolaires de l'ASQ,
► Les alarmes de catégorie « Signatures contextuelles » : associées aux analyses des signatures contextuelles.

Le module d'analyse par Signatures Contextuelles fait l'objet d'une licence supplémentaire payante.

© Copyright NETASQ 2006

Alarmes protocolaires



La grille se divise en six colonnes :

► la catégorie : les alarmes sont regroupées par catégorie qui sont : IP, TCP, UDP ICMP, IGMP, misc, DoS, scan, DNS, FTP, HTTP,

► l'action : lorsqu'une alarme est remontée le paquet qui a provoqué cette alarme subit l'action associée. Elle peut être « bloque » ou passe. Une case grisée indique qu'aucune modification de l'action n'est possible,

► la réaction : en plus de l'action associée à l'alarme, il est possible de définir une réaction à la remontée d'une alarme parmi l'envoi d'un mail, la mise en quarantaine de la machine responsable ou aucune réaction.

► Envoi d'un mail : lorsque le service d'envoi des mails est activé (Voir « Configuration du service Mail ») il est possible de définir l'envoi d'un mail lorsque deux facteurs sont réunis : le nombre de fois où l'alarme a été remontée et dans quel intervalle de temps.

► Mise en quarantaine : cette mise en quarantaine permet de bloquer l'ensemble des trafics en provenance de la machine responsable de la remontée d'alarme. Cette quarantaine dynamique est associée à une durée (en minutes) et ne résiste pas au redémarrage (la liste des machines en quarantaine est réinitialisée lors d'un redémarrage de l'IPS-Firewall).

► Détail : cette option permet de sauvegarder le paquet responsable de la remontée d'alarme. La taille des informations sauvegardées dépend du modèle de votre IPS-Firewall. Ce paquet est alors visualisable grâce au Moniteur Temps réel. (Voir « Moniteur Temps Réel »).

► le niveau : trois niveaux d'alarmes sont disponibles, ignore, minor et major,

► le message : cela correspond à l'intitulé de l'alarme. Des informations complémentaires sur l'alarme sont disponibles directement dans le firewall manager grâce aux liens présents dans cette colonne. La base des alarmes NETASQ recensant toutes les alarmes est disponible dans la documentation associée à la suite d'administration.

Profils de protection

Le bouton « Configuration par défaut » vous permet de redéfinir la configuration des alarmes selon trois profils de protection disponibles (faible, moyen fort).

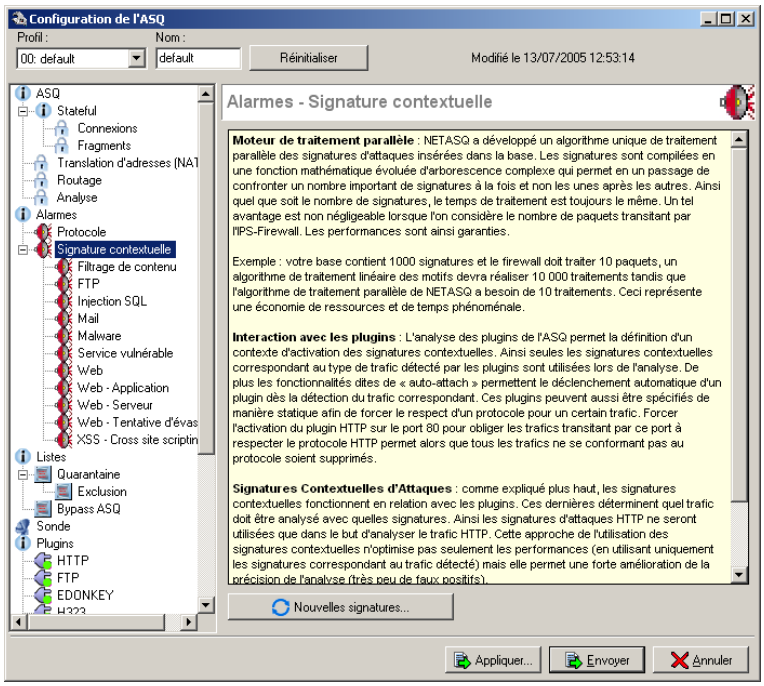
Aide en ligne

Chaque alarme protocolaire est associée à une explication fournie par NETASQ au moyen d'une page HTML intégrée dans l'application Firewall Manager. Pour afficher l'aide en ligne d'une alarme protocolaire, reportez-vous à la procédure suivante :

1. Sélectionnez l'alarme protocolaire dont vous souhaitez l'explication ;

2. Cliquez sur l'option « Montrer l'aide » pour afficher l'aide correspondante à l'alarme protocolaire sélectionnée.

Signatures contextuelles


Configuration de l'ASQ
Profil :
Nom :
00: default
default
Réinitialiser
Modifié le 13/07/2005 12:53:14
ASQ
Stateful
Connexions
Fragments
Translation d'adresses (NAT
Routage
Analyse
Alarmes
Protocole
Signature contextuelle
Filtrage de contenu
FTP
Injection SQL
Mail
Malware
Service vulnérable
Web
Web - Application
Web - Serveur
Web - Tentative d'évas
XSS - Cross site scriptin
Listes
Quarantaine
Exclusion
Bypass ASQ
Sonde
Plugins
HTTP
FTP
EDONKEY
Alarmes - Signature contextuelle
Moteur de traitement parallèle : NETASQ a développé un algorithme unique de traitement parallèle des signatures d'attaques insérées dans la base. Les signatures sont compilées en une fonction mathématique évoluée d'arborescence complexe qui permet en un passage de confronter un nombre important de signatures à la fois et non les unes après les autres. Ainsi quel que soit le nombre de signatures, le temps de traitement est toujours le même. Un tel avantage est non négligeable lorsque l'on considère le nombre de paquets transitant par l'IPS-Firewall. Les performances sont ainsi garanties.
Exemple : votre base contient 1000 signatures et le firewall doit traiter 10 paquets, un algorithme de traitement linéaire des motifs devra réaliser 10 000 traitements tandis que l'algorithme de traitement parallèle de NETASQ a besoin de 10 traitements. Ceci représente une économie de ressources et de temps phénoménale.
Interaction avec les plugins : L'analyse des plugins de l'ASQ permet la définition d'un contexte d'activation des signatures contextuelles. Ainsi seules les signatures contextuelles correspondant au type de trafic détecté par les plugins sont utilisées lors de l'analyse. De plus les fonctionnalités dites de « auto-attach » permettent le déclenchement automatique d'un plugin dès la détection du trafic correspondant. Ces plugins peuvent aussi être spécifiés de manière statique afin de forcer le respect d'un protocole pour un certain trafic. Forcer l'activation du plugin HTTP sur le port 80 pour obliger les trafics transitant par ce port à respecter le protocole HTTP permet alors que tous les trafics ne se conformant pas au protocole soient supprimés.
Signatures Contextuelles d'Attaques : comme expliqué plus haut, les signatures contextuelles fonctionnent en relation avec les plugins. Ces dernières déterminent quel trafic doit être analysé avec quelles signatures. Ainsi les signatures d'attaques HTTP ne seront utilisées que dans le but d'analyser le trafic HTTP. Cette approche de l'utilisation des signatures contextuelles n'optimise pas seulement les performances (en utilisant uniquement les signatures correspondant au trafic détecté) mais elle permet une forte amélioration de la précision de l'analyse (très peu de faux positifs).
Nouvelles signatures...
Appliquer...
Envoyer
Annuler

Les attaques correspondant à des erreurs d'implémentation locales clientes ou serveurs sont bloquées par le module de détection et de prévention d'intrusion par signatures contextuelles. Cette base complémentaire aux autres analyses permet d'affiner l'analyse globale du trafic réalisé par l'IPS-Firewall NETASQ en gommant les inconvénients des systèmes des pattern matching habituels (comme les IDS) comme, par exemple, les faux positifs. De plus, grâce à la sauvegarde du contexte, le système NETASQ est plus efficace.

Les signatures contextuelles de l'ASQ sont divisées dans l'interface graphique du Firewall Manager selon les fonctions qu'elles réalisent, les attaques qu'elles préviennent ou les trafics qu'elles surveillent. Dans la version 6.1, les signatures contextuelles sont divisées en de nombreuses catégories : Filtrage de contenu, Mail, WEB, Cross Site Scripting, FTP, Malware, SQL injection, Services vulnérables…

De la même façon que pour les alarmes protocolaires, la grille se divise en six colonnes :

► la catégorie : les alarmes sont regroupées par contexte. Ainsi les signatures s'appliquent que dans un certain contexte ce qui permet de baisser le nombre de faux positifs et d'obtenir de meilleures performances.

► l'action : lorsqu'une alarme est remontée le paquet qui a provoqué cette alarme subit l'action associée. Elle peut être « bloque » ou passe. Une case grisée indique qu'aucune modification de l'action n'est possible,

► la réaction : en plus de l'action associée à l'alarme, il est possible de définir une réaction à la remontée d'une alarme parmi l'envoi d'un mail, la mise en quarantaine de la machine responsable ou aucune réaction.

► Envoi d'un mail : lorsque le service d'envoi des mails est activé (Voir « Configuration du service Mail ») il est possible de définir l'envoi d'un mail lorsque deux facteurs sont réunis : le nombre de fois où l'alarme a été remontée et dans quel intervalle de temps.

► Mise en quarantaine : cette mise en quarantaine permet de bloquer l'ensemble des trafics en provenance de la machine responsable de la remontée d'alarme. Cette quarantaine dynamique est associée à une durée (en minutes) et ne résiste pas au redémarrage (la liste des machines en quarantaine est réinitialisée lors d'un redémarrage de l'IPS-Firewall).

► Détail : cette option permet de sauvegarder le paquet responsable de la remontée d'alarme. La taille des informations sauvegardées dépend du modèle de votre IPS-Firewall. Ce paquet est alors visualisable grâce au Moniteur Temps réel. (Voir « Moniteur Temps Réel »).

► le niveau : trois niveaux d'alarmes sont disponibles, ignore, minor et major,

► nouveau : ce paramètre indique la signature contextuelle est nouvelle dans la liste des signatures contextuelles téléchargée sur le site WEB NETASQ. Cette signature contextuelle reste validée « Nouveau » tant que l'administrateur ne l'a pas décochée.

► le message : cela correspond à l'intitulé de l'alarme. Des informations complémentaires sur l'alarme sont disponibles directement dans le firewall manager grâce aux liens présents dans cette colonne. La base des alarmes NETASQ recensant toutes les alarmes est disponible dans la documentation associée à la suite d'administration.

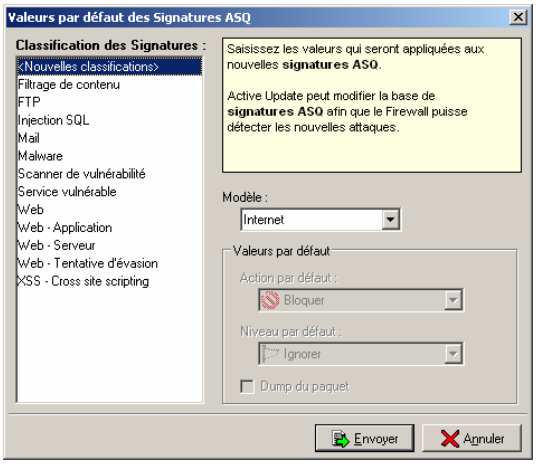
Profils de protection

Le bouton « Configuration par défaut » vous permet de redéfinir la configuration des alarmes selon trois profils de protection disponibles (faible, moyen, fort ou Internet). Le profil « Internet » est notamment tout à fait adapté à la prévention des menaces en provenance d'Internet.

Nouvelles signatures

La bonne configuration des signatures contextuelles, notamment en terme d'actions (remontées d'alarmes, blocage des trafics associés…), garantit la pertinence de l'action de l'IPS-Firewall sur les trafics surveillés par ces signatures et la sécurité des ressources que l'IPS-Firewall protège. Or ces signatures contextuelles sont régulièrement mises à jour par NETASQ et la gestion des actions entreprises par ces signatures est fastidieuse pour l'administrateur car il doit vérifier régulièrement l'apparition de nouvelles signatures et configurer l'action de celles-ci.

Ainsi l'option « Nouvelles signatures » du sous-menu « Signatures contextuelles » permet une « pré-configuration » du comportement des futures signatures contextuelles qui seront téléchargées lors du processus de mise à jour de la base de signatures contextuelles. Cette pré-configuration s'effectue par catégorie. Toutes les signatures appartenant à une catégorie donnée seront configurées avec les paramètres définis par l'administrateur.



Le tableau suivant indique les options du menu « Nouvelles signatures » :

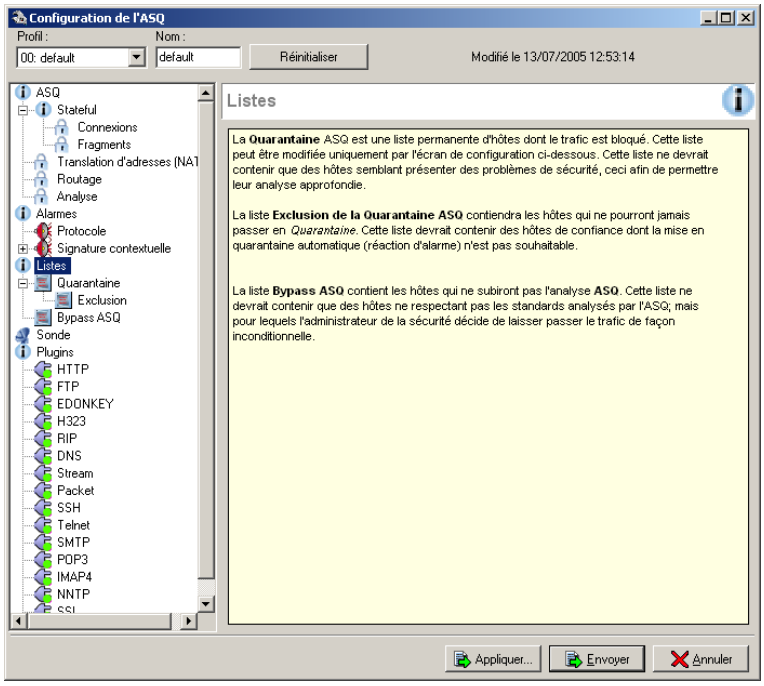
Classification des signatures	La pré-configuration du comportement des futures signatures s'effectue par catégorie. La liste présentée par le champ « Classification des signatures » désigne l'ensemble des catégories doivent être configurées. La catégorie « Nouvelles catégories » fait référence aux catégories de signatures contextuelles qui n'existent pas encore.
Modèle	Tel que pour les signatures déjà téléchargées, il est possible d'appliquer pour les futures signatures, un modèle ou profil de protection parmi faible, moyen, fort, internet ou personnalisé. Pour le modèle personnalisé, l'administrateur doit définir les actions par défaut associées à ces nouvelles signatures contextuelles.
Valeurs par défaut	Disponibles uniquement lors de la définition d'un modèle personnalisé, ces options permettent la définition des actions par défaut (action : bloquer ou passer, niveau : majeur, mineur ou ignorer et le dump du paquet) associées aux nouvelles signatures de la catégorie sélectionnée.

Aide en ligne

Chaque signature contextuelle est associée à une explication fournie par NETASQ au moyen d'une page HTML intégrée dans l'application Firewall Manager. Pour afficher l'aide en ligne d'une signature contextuelle, reportez-vous à la procédure suivante :

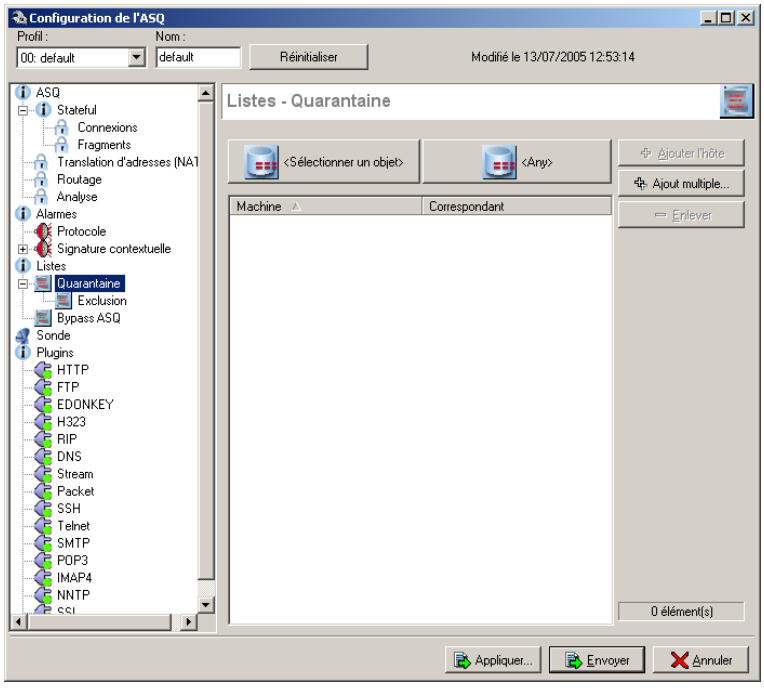
1. Sélectionnez la signature contextuelle dont vous souhaitez l'explication ;

2. Cliquez sur l'option « Montrer l'aide » pour afficher l'aide correspondante à la signature contextuelle sélectionnée.


Configuration de l'ASQ
Profil :
Nom :
00: default
default
Réinitialiser
Modifié le 13/07/2005 12:53:14
ASQ
Stateful
Connexions
Fragments
Translation d'adresses (NAT
Routage
Analyse
Alarmes
Protocole
Signature contextuelle
Listes
Quarantaine
Exclusion
Bypass ASQ
Sonde
Plugins
HTTP
FTP
EDONKEY
H323
RIP
DNS
Stream
Packet
SSH
Telnet
SMTP
POP3
IMAP4
NNTP
Listes
La Quarantaine ASQ est une liste permanente d'hôtes dont le trafic est bloqué. Cette liste peut être modifiée uniquement par l'écran de configuration ci-dessous. Cette liste ne devrait contenir que des hôtes semblant présenter des problèmes de sécurité, ceci afin de permettre leur analyse approfondie.
La liste Exclusion de la Quarantaine ASQ contiendra les hôtes qui ne pourront jamais passer en Quarantaine. Cette liste devrait contenir des hôtes de confiance dont la mise en quarantaine automatique (réaction d'alarme) n'est pas souhaitable.
La liste Bypass ASQ contient les hôtes qui ne subiront pas l'analyse ASQ. Cette liste ne devrait contenir que des hôtes ne respectant pas les standards analysés par l'ASQ, mais pour lequels l'administrateur de la sécurité décide de laisser passer le trafic de façon inconditionnelle.
Appliquer...
Envoyer
Annuler

Ce menu de la configuration de l'ASQ est divisé en deux parties les listes noires et les listes blanches.

Quarantaine



Ce menu vous permet de configurer une quarantaine statique (cette quarantaine est différente de la quarantaine dynamique évoquée plus haut, Voir « Quarantaine dynamique »). Cette quarantaine

permet d'interdire tous les trafics en provenance d'une machine, à destination d'une machine ou entre deux machines.

Le menu de configuration des listes noires se présente sous la forme d'une grille représentant les hôtes et leur correspondant (si cela est nécessaire) actuellement en liste noire.

Pour ajouter une entrée dans cette grille, suivez la procédure suivante :

1. Sélectionnez l'hôte que vous désirez mettre en quarantaine statique grâce au bouton « Hôte » de la barre d'action située au bas du menu,

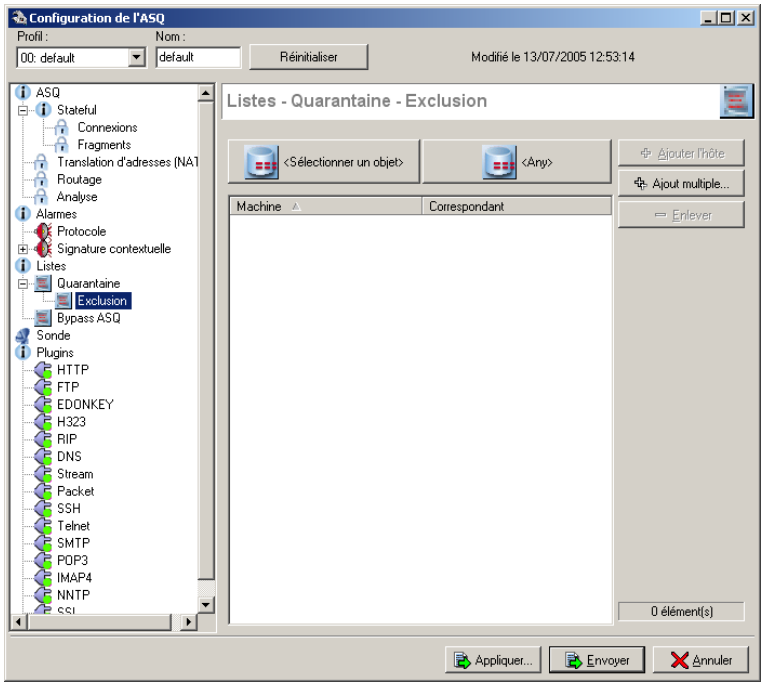
2. Sélectionnez l'hôte correspondant pour la mise en quarantaine (tous les trafics, dans les deux sens, entre ces machines seront interdits). Si vous désirez interdire tous les trafics vers (ou en provenance) de n'importe quelle autre machine, veuillez laisser le champ « Hôte correspondant » vide,

3. Ajoutez l'entrée en sélectionnant le bouton « Ajouter l'hôte ».

Le bouton « Enlever » vous permet de supprimer l'entrée sélectionnée.

Le bouton « Ajout multiple » vous permet de sélectionner simultanément plusieurs hôtes à placer en liste noire. Ce bouton ajoutera alors une entrée qui interdit les trafics entre l'hôte et toutes les autres machines.

Exclusion



Ce menu permet d'exclure une machine d'un groupe qui aurait été mis en quarantaine statique.

Le menu de configuration des exclusion de listes noires se présente sous la forme d'une grille représentant les hôtes et leur correspondant (si cela est nécessaire) actuellement en exclus de la liste noire.

Pour ajouter une entrée dans cette grille, suivez la procédure suivante :

1. Sélectionnez l'hôte que vous désirez exclure de la quarantaine statique grâce au bouton « Hôte » de la barre d'action située au bas du menu,

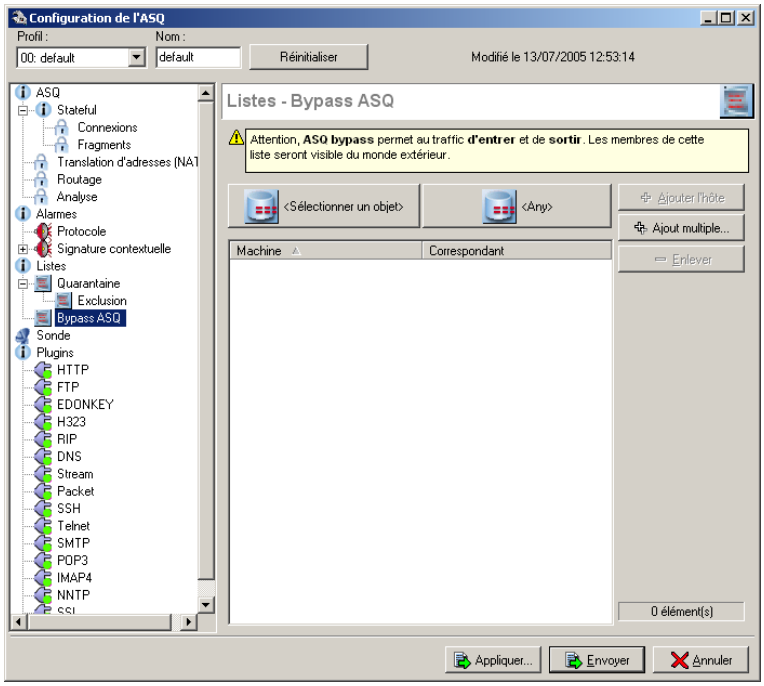
2. Sélectionnez l'hôte correspondant pour l'exclusion de la quarantaine (tous les trafics, dans les deux sens, entre ces machines ne seront pas interdits). Si vous désirez ne pas interdire tous les trafics vers (ou en provenance) de n'importe quelle autre machine, veuillez laisser le champ « Hôte correspondant » vide,

3. Ajoutez l'entrée en sélectionnant le bouton « Ajouter l'hôte ».

Le bouton « Enlever » vous permet de supprimer l'entrée sélectionnée.

Le bouton « Ajout multiple » vous permet de sélectionner simultanément plusieurs hôtes à placer exclusion de liste noire. Ce bouton ajoutera alors une entrée qui permettra d'exclure de la liste noire les trafics entre l'hôte et toutes les autres machines.

Bypass ASQ



Ce menu vous permet de configurer une liste blanche de machines. Autrement appelée Bypass, cette liste de contournement de l'ASQ permet de définir les trafics qui ne doivent pas être soumis à l'analyse de l'ASQ.

La configuration d'une liste blanche de machines entraine une très forte diminution de la sécurité des ressources et infrastructures protégées par l'IPS-Firewall. En effet AUCUNE analyse ni politique de filtrage n'est appliquée au trafic concerné par la liste blanche (dans les deux sens).

Le menu de configuration des listes blanches se présente sous la forme d'une grille représentant les hôtes et leur correspondant (si cela est nécessaire) actuellement en liste blanche.

Pour ajouter une entrée dans cette grille, suivez la procédure suivante :

1. Sélectionnez l'hôte que vous désirez mettre en liste blanche grâce au bouton « Hôte » de la barre d'action située au bas du menu,

2. Sélectionnez l'hôte correspondant pour la mise en liste blanche (tous les trafics, dans les deux sens, entre ces machines ne seront pas analysés par l'ASQ). Si vous désirez contourner l'analyse de l'ASQ pour tous les trafics vers (ou en provenance) de n'importe quelle autre machine, veuillez laisser le champ « Hôte correspondant » vide,

3. Ajoutez l'entrée en sélectionnant le bouton « Ajouter l'hôte ».

Le bouton « Enlever » vous permet de supprimer l'entrée sélectionnée.

© Copyright NETASQ 2006

Le bouton « Ajout multiple » vous permet de sélectionner simultanément plusieurs hôtes à placer en liste blanche. Ce bouton ajoutera alors une entrée qui contourne l'ASQ pour les trafics entre l'hôte et toutes les autres machines.

Exclusion

Ce menu permet d'interdire qu'une machine soit placée en liste blanche.

Le menu de configuration des exclusion de listes blanches se présente sous la forme d'une grille représentant les hôtes et leur correspondant (si cela est nécessaire) actuellement en exclus de la liste blanche.

Pour ajouter une entrée dans cette grille, suivez la procédure suivante :

1. Sélectionnez l'hôte que vous désirez exclure de la liste blanche grâce au bouton « Hôte » de la barre d'action située au bas du menu,

2. Sélectionnez l'hôte correspondant pour l'exclusion de la liste blanche. Si vous désirez interdire que tous les trafics vers (ou en provenance) de n'importe quelle autre machine soit placés en liste blanche, veuillez laisser le champ « Hôte correspondant » vide,

3. Ajoutez l'entrée en sélectionnant le bouton « Ajouter l'hôte ».

Le bouton « Enlever » vous permet de supprimer l'entrée sélectionnée.

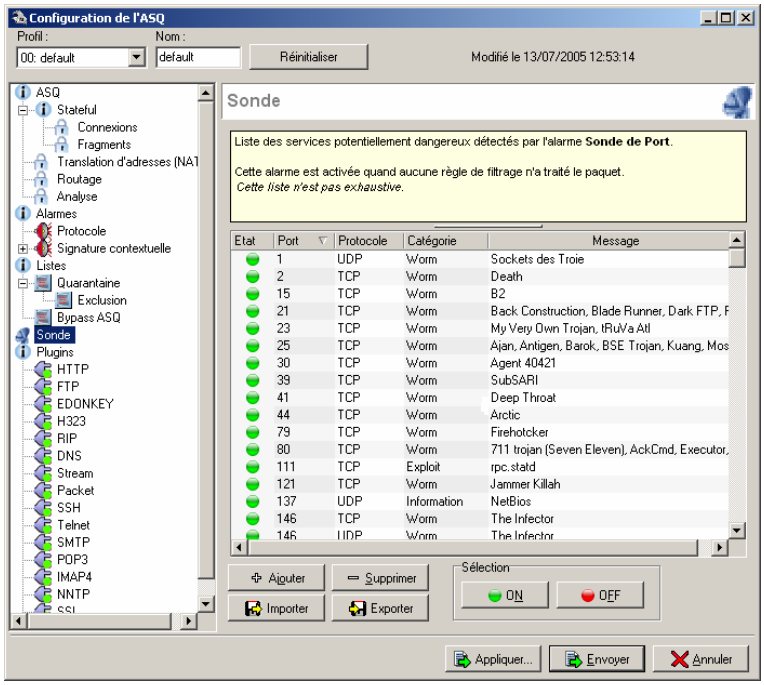
Le bouton « Ajout multiple » vous permet de sélectionner simultanément plusieurs hôtes à placer exclusion de liste blanche. Ce bouton ajoutera alors une entrée qui permettra d'exclure de la liste blanche les trafics entre l'hôte et toutes les autres machines.

Priorité en liste noire, liste blanche et filtrage.

Un paquet (pas de notion de sens) est systématiquement refusé s'il correspond à une entrée de la liste noire, quelle que soit la liste blanche et la politique de filtrage.

La vérification de liste noire faite, un paquet absent (de la liste noire) est systématiquement autorisé s'il correspond à une entrée dans la liste blanche, quelle que soit la politique de filtrage, sans passer par les analyses de l'ASQ (protocolaires et signatures contextuelles).

© Copyright NETASQ 2006



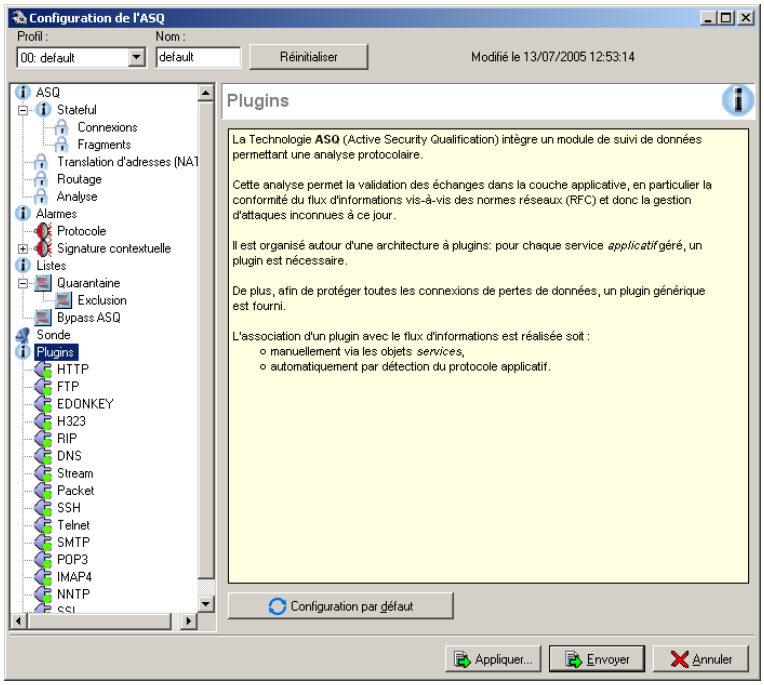
Les paramètres de configuration du module Probe sont modifiables dans l'onglet « Sonde » du menu ASQ de l'arborescence.

Ce menu présente une liste de services potentiellement dangereux utilisés fréquemment par des chevaux de Troie notamment ou des vers. Lorsqu'un de ces services est utilisé cela remonte l'alarme « Sonde de port » si et seulement si aucune règle de filtrage n'est associé au paquet en question. Le paquet descend la liste des règles sans être traité.

Grâce aux boutons d'action au bas de la fenêtre vous pouvez modifier cette liste suivant les ports que vous désirez surveiller. La grille se divise en cinq parties :

- ► l'état : pour désactiver, sans supprimer la sonde de ce port,
- ► le port : le numéro du port à surveiller,
- ► le protocole : le protocole véhiculant des paquets malveillants
- ► la catégorie : plusieurs catégories sont disponibles (exploit, worm, p2p, relaying, …)
- ► le message : un commentaire que vous pouvez indiquer librement.

© Copyright NETASQ 2006



La nouveauté de la nouvelle version de l'ASQ est son architecture optimisée à plugins protocolaires. Ces plugins réalisent une étude approfondie des données qui transitent dans les paquets, notamment en vérifiant leur cohérence par rapport aux entêtes, aux protocoles correspondants.

Les paramètres de configuration des plugins protocolaires sont modifiables dans l'onglet « Plugins » du menu ASQ de l'arborescence.

Les fonctionnalités disponibles pour les plugins actuels sont présentées dans le tableau suivant :

Etat	Activation ou désactivation du plugin.
Activation automatique	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage.
Fermer la connexion à l'attachement du plugin	Lorsque le plugin s'active automatiquement sur un trafic, la connexion qui a déclenchée l'activation automatique du trafic est fermée. Les paquets sont alors bloqués.
Traces	Activation ou désactivation de la remontée des logs concernant le plugin.
Shout Cast (HTTP uniquement)	Support du Shout Cast.
Webdav (HTTP uniquement)	Support du WebDav.
RFC 775 (FTP uniquement)	Respect et support des fonctionnalités de parcours des répertoires du protocole FTP.
Authentification SSL (FTP uniquement)	Activation du support de l'authentification SSL pour la protocole FTP.

© Copyright NETASQ 2006

Pas de validation d'authentification	Cette option permet de rendre la séquence d'authentification sur un serveur FTP, facultative.

Les tampons du plugin HTTP (Onglet Propriétés)

La gestion des débordements de tampons (ou Buffer Overflow) est primordiale chez NETASQ, c'est pourquoi la définition des tailles maximales permises pour les tampons dans le cadre du protocole HTTP est particulièrement développée.

Tampon URL	Nombre maximum d'octets pour l'URL incluant les attributs de formatage.
Tampon BODY	Nombre maximum d'octets pour le champ BODY incluant les attributs de formatage.
Tampon COOKIE	Nombre maximum d'octets pour le champ COOKIE incluant les attributs de formatage.
Tampon HOST	Nombre maximum d'octets pour le champ HOST incluant les attributs de formatage.
Tampon CONTENTTYPE	Nombre maximum d'octets pour le champ CONTENTTYPE incluant les attributs de formatage.
Tampon AUTHORIZATION	Nombre maximum d'octets pour le champ AUTHORIZATION incluant les attributs de formatage.
Opérations autorisées	Liste des commandes HTTP autorisées, séparées par des virgules. Longueur maximum de 128 caractères.
Opérations interdites	Liste des commandes HTTP interdites, séparées par des virgules. Longueur maximum de 128 caractères.

Les tampons du plugin FTP (Onglet Propriétés)

Les différents tampons FTP pouvant être gérés sont indiqués dans le tableau suivant :

Tampon LINE	Nombre maximum d'octets pour une ligne FTP incluant les attributs de formatage.
Tampon PASS	Nombre maximum d'octets pour le mot de passe FTP incluant les attributs de formatage.
Tampon PATH	Nombre maximum d'octets pour le chemin FTP incluant les attributs de formatage.
Tampon SITE	Nombre maximum d'octets pour le SiteString FTP incluant les attributs de formatage.
Tampon USER	Nombre maximum d'octets pour le nom d'utilisateur FTP incluant les attributs de formatage.
Opérations autorisées	Liste des commandes FTP autorisées, séparées par des virgules. Longueur maximum de 128 caractères.
Opérations interdites	Liste des commandes FTP interdites, séparées par des virgules. Longueur maximum de 128 caractères.

Les tampons du plugin DNS (Onglet Propriétés)

Les différents tampons DNS pouvant être gérés sont indiqués dans le tableau suivant :

Tampon NAME	Nombre maximum d'octets pour le champ NAME d'une requête DNS.

Particularité des plugins « Stream » et « Packet »

Ces plugins permettent la vérification des données liées à aucun protocole en particulier. Cette option, une fois activée, n'est utilisée par le firewall que si aucun autre plugin ne s'active lors de l'analyse du paquet en question. Cette option est cochée par défaut pour vous offrir un maximum de sécurité, l'inconvénient est que les performances du firewall en sont réduites. Vous pouvez désactiver cette option, cela aura pour conséquence de garantir de meilleures performances mais la sécurité de vos données sera moindre. Le plugin « Stream » est associé au protocole TCP et le plugin « Packet » à l'UDP.

Chapitre IV

NAT, filtrage et QoS

© Copyright NETASQ 2006

Section A

Translation d'adresses

© Copyright NETASQ 2006

Pour cette section, vous devez avoir franchi les étapes

► Installation, pré-configuration, intégration,
► Configuration réseau,
► Configuration des objets.

Pour cette section, vous devez connaître

► Les machines dont vous souhaitez translater l'adresse IP.

Utilité de la section

Cette section vous permet de définir les objets dont vous voulez translater l'adresse.

Accéder à cette section

Accédez à la boîte de dialogue par le menu « Politique > NAT » de l'arborescence de l'interface graphique.

Vous devez être connecté avec les privilèges de modification pour pouvoir effectuer ces modifications.

Avant d'effectuer toute modification importante sur votre Firewall NETASQ, nous vous conseillons d'effectuer une sauvegarde. Ainsi, en cas de mauvaise manipulation vous pourrez vous retrouver dans l'état précédent. Pour plus d'informations sur les sauvegardes, veuillez vous référer au chapitre Sauvegardes et Mise à jour.

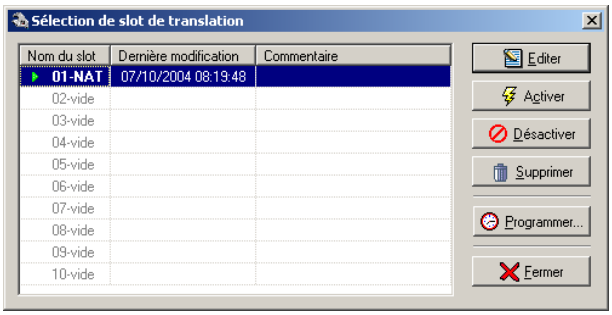
Introduction à cette section

Les tables de translation d'adresses sont stockées sur le Firewall NETASQ dans des slots (fichiers de configuration numérotés de 01 à 10).

Chaque slot peut être programmé à une heure précise de la semaine, en écrasant la configuration du slot précédemment activé.

© Copyright NETASQ 2006

Lorsque vous sélectionner le sous menu « Politique > NAT » une boîte de dialogue s'affiche, elle vous permet de manipuler les slots associés à la translation d'adresses.



Elle est découpée en deux zones :

Gauche	Liste des slots.
Droite	Actions sur le slot sélectionné.

Liste des slots

Dans cette partie de la boite de dialogue se trouve la liste des slots. Il en existe 10, numérotés de 01 à 10.

Chaque slot possède un nom, une date/heure de mise en activité et la date de dernière modification effectuée sur ce slot. La programmation de l'activation de ces slots se fait grâce au programmateur horaire (Section D « programmateur horaire »).

Le slot en cours d'activité est indiqué par une petite flèche verte à gauche de son nom. Un slot est dit "en activité" lorsque les paramètres qu'il contient sont en service. Il ne peut y avoir plus d'un slot en activité car les paramètres du dernier slot activé écrasent ceux du slot activé précédemment.

Si vous modifiez un slot, vous devez le réactiver pour prendre en compte les modifications. Un slot modifié mais non réactivé est notifié par l'icône à la place de la flèche verte habituelle.

Il est possible qu'il n'y ait aucun slot en activité, cela implique qu'aucune translation d'adresses n'est active.

Chaque slot ne doit pas obligatoirement contenir des paramètres.

Un slot pour lequel il n'existe pas de fichier de configuration sur le Firewall NETASQ est affiché sous le nom « vide » dans la liste.

Un slot est dit sélectionné quand vous faites un simple clic de la souris sur son nom. La sélection faite, vous pouvez l'éditer ou l'activer.

© Copyright NETASQ 2006

Actions sur le slot sélectionné

Quand un slot est sélectionné, vous pouvez réaliser différentes actions :

Editer	Modifier les règles de translation d'adresses associées à ce slot.
Activer	Activer immédiatement un slot : les paramètres enregistrés dans ce slot écrasent les paramètres en vigueur. Lorsqu'on sélectionne un slot déjà activé ce bouton ce transforme en un bouton « désactiver » pour réaliser l'action de désactivation.
Programmer	Donner l'heure et le ou les jours auxquels le fichier va s'activer automatiquement.
Effacer	Efface le slot et toutes ses informations.
Désactiver	Désactive le slot actuellement activé. Aucune translation d'adresse n'est alors effectuée.
Fermer	Retour à l'écran principal.

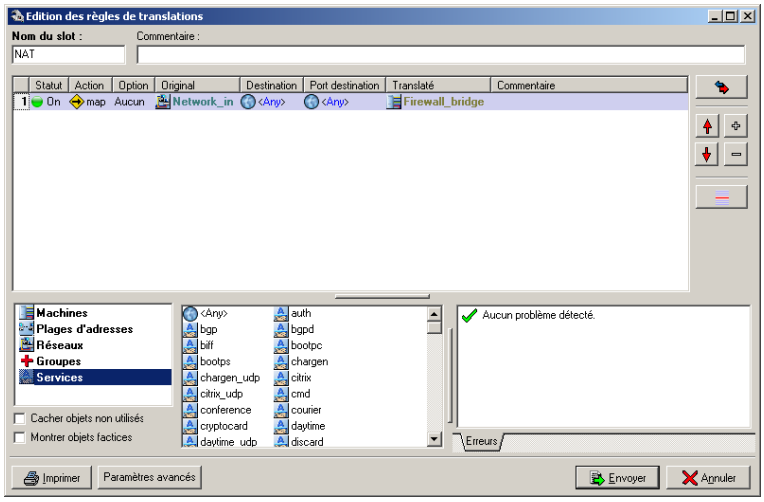
© Copyright NETASQ 2006

Edition d'un slot de translation

Reportez-vous à la procédure suivante pour éditer un slot de translation :

1. Sélectionnez un slot dans la liste des slots de translation,

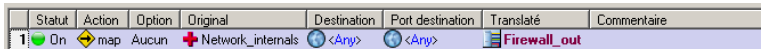
2. Cliquez sur le bouton « Editer » de la boite de dialogue contenant la liste des slots de translation.



La fenêtre d'édition d'un slot de translation apparaît. Elle est composée de plusieurs parties :

► Une zone comportant les règles de translation sous la forme d'un tableau ;
► Un menu « Drag'n Drop » ;
► Un analyseur de cohérence et de conformité des règles ;
► Une zone d'actions possibles.

Règles de translation



Statut	La règle est utilisée par l'IPS-Firewall NETASQ, La règle est désactivée.
Action	Définit le type de translation que vous désirez effectuer. La translation peut être unidirectionnelle, bidirectionnelle, une redirection ou un partage de charge et s'effectuer entre toutes les interfaces du Firewall.
Option	Les options permettent d'ajouter deux types de services particuliers, FTP actif (DOS) et Real Audio (anciennes versions), qui font figurer les adresses sources dans les champs de données des paquets TCP/IP. Ces services nécessitent donc un traitement particulier lors de la translation d'adresses.
Original Source	Adresse IP non translatée. Un double clic sur cette zone permet de choisir l'objet associé. Le sélecteur d'objets n'affiche que les objets disponibles pour ce champ.
Destination	Destination du trafic qui nécessite une translation. Un double clic sur cette zone permet de choisir l'objet associé. Le sélecteur

© Copyright NETASQ 2006

	d'objets n'affiche que les objets disponibles pour ce champ.
Port de destination	Port de destination du trafic qui nécessite une translation. Un double clic sur cette zone permet de choisir l'objet associé. Le sélecteur d'objets n'affiche que les objets disponibles pour ce champ.
Translaté	Adresse IP translatée (modifiée par le firewall). Un double clic sur cette zone permet de choisir l'objet associé. Le sélecteur d'objets n'affiche que les objets disponibles pour ce champ.
Commentaires	Commentaires que vous pouvez associer à cette règle de translation.

En exemple, on peut indiquer que tout le trafic de l' « original source », à destination du port « Port de la destination » de la machine « Destination », est redirigé vers la machine « translaté ».

Lorsqu'un icône ressemblant à un point d'interrogation dans un cercle rouge apparaît dans un champ cela signifie que ce champ est obligatoire pour la règle de translation.

Attention, n'activez les options que si vous êtes sûrs de vouloir utiliser ces services. Ils ralentissent le traitement des paquets et peuvent être source de conflits.

Mode Avancé

L'affichage détaillé permet d'accéder aux colonnes interfaces et port translaté. Pour obtenir l'affichage détaillé, cliquez sur le bouton « Mode Avancé » .

Interface	Interface sur laquelle s'applique la règle de translation. Par défaut, le firewall la sélectionne automatiquement en fonction de l'opération et des adresses IP source et destination. Il est possible de la modifier pour appliquer la règle sur une autre interface.
Port translaté	Port vers lequel est faite la translation. Surtout utilisé pour préciser une plage de port vers lesquels s'effectue la translation d'adresse unidirectionnelle ou pour réaliser de la translation de port (pour rediriger une connexion demandée sur le port XX vers le port YY). Un double clic sur cette zone permet de choisir l'objet associé. Le sélecteur d'objets n'affiche que les objets disponibles pour ce champ.

Opération

Cette zone de la boîte de dialogue contient une grille vous permettant de définir les translations d'adresses à appliquer. Les différentes possibilités (Opération) sont :

Translation unidirectionnelle (map)

La translation d'adresses unidirectionnelle vous permet de convertir des adresses IP réelles de vos réseaux (interne, externe ou DMZ) en une adresse IP virtuelle sur un autre réseau (interne, externe ou DMZ) lors du passage par le firewall. L'adresse source est changée en adresse destination uniquement si la connexion provient de la machine source (unidirectionnelle).

La translation unidirectionnelle est généralement utilisée pour masquer les adresses IP en sortie du firewall.

Il faut préciser la plage de ports translatés en affichage détaillé pour éviter les conflits de ports.

Les plages d'adresse sont supportées par l'action « map ». Une fois que les ports de la première adresse sont tous utilisés, les ports de la seconde adresse sont utilisés…

Définition de la règle

Indiquez en origine l'adresse IP réelle (privée) de la machine ou du réseau, et en adresse translatée l'adresse IP virtuelle que vous désirez affecter.

No map

Il est possible de retirer une machine, comprise dans un réseau translaté, de l'opération de translation de type map.

L'adresse de cette machine ne sera alors pas translatée au travers du firewall.

Définition de la règle

L'origine est la machine qui ne doit pas être translatée. Choisissez l'option no map et n'indiquez rien dans la colonne "Translaté".

Cette règle doit forcément être suivie d'une règle de type map.

Pour une règle no map, vous devez spécifier l'interface du firewall sur laquelle l'opération de no map sera effectuée (cette interface est la même que pour l'opération map associée).

Vous pouvez consulter les Exemples de configurations de translation d'adresses en Annexe pour une meilleure compréhension de ces choix.

Translation bidirectionnelle (map bidirectionnel)

La translation d'adresses bidirectionnelle vous permet de convertir une adresse IP (ou N adresses IP) en une autre (ou en N adresses IP) lors du passage par le firewall, quelle que soit la provenance de la connexion.

Pour une règle de bi-map de N vers N, les plages d'adresses, réseaux ou groupes d'hôtes original et translaté doivent être de même taille.

La translation bidirectionnelle est généralement utilisée pour donner accès à un serveur depuis l'extérieur avec une adresse IP publique qui n'est pas l'adresse réelle de la machine.

Les plages d'adresses sont supportées par l'action « bi-map ». Les adresses sources et translatées sont utilisées dans l'ordre : la plus « petite » adresse du champ source est translaté vers la plus « petite » adresse du champ translaté.

Définition de la règle

L'adresse IP origine correspond à l'adresse physique de la machine et l'adresse IP translatée à l'adresse IP virtuelle utilisée.

© Copyright NETASQ 2006

Redirection de port (redirection)

La redirection de port permet de rediriger les paquets en provenance d'une ou plusieurs sources à destination d'une ou plusieurs adresses IP avec un port identique vers une autre adresse IP/ N° de port.

Ceci permet de rediriger le flux vers la machine concernée, à partir d'une seule adresse IP publique, en fonction du numéro de port.

Les numéros de port sont accessibles en affichage détaillé.

Définition de la règle

L'adresse IP publique utilisée correspond à l'adresse origine et l'adresse de redirection à l'adresse translatée.

Partage de charge (split)

Le partage de charge redirige les flux à destination d'une adresse IP vers plusieurs machines (groupe de machines). Il est possible de préciser les ports des adresses à rediriger en affichage détaillé.

Dans cette version, le partage est fait séquentiellement, sans vérifier l'accessibilité des machines.

Définition de la règle

Le pool d'adresses IP utilisé (groupe de machines) correspond à la partie translatée, l'origine étant l'adresse IP à contacter.

Vous pouvez consulter les Exemples de configurations de translation d'adresses en Annexe pour une meilleure compréhension de ces choix.

Actions possibles

Nom du slot	Nom donné au fichier de configuration.
Commentaire	Commentaire indicatif associé au slot de translation.
Mode avancé	Affichage des paramètres de configuration avancés de la translation d'adresses.
Insérer	Insérer une ligne vierge après la ligne sélectionnée.
Effacer	Supprimer la ligne sélectionnée.
Flèche vers le haut	Placer la ligne sélectionnée avant la ligne directement au dessus.
Flèche vers le bas	Placer la ligne sélectionnée après la ligne directement en dessous.
Insérer un séparateur	Cette option permet d'insérer un séparateur au dessus de la ligne sélectionnée afin d'indiquer un commentaire sur une ligne de l'édition de la translation d'adresses. Pour définir un séparateur, il s'agit d'indiquer un commentaire et une couleur pour ce séparateur.

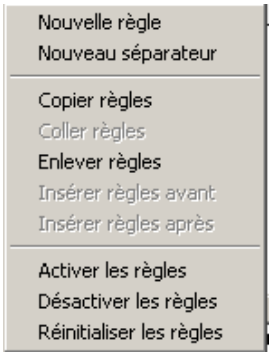
Imprimer	Ouvrir la boîte de dialogue d'Impression permettant d'imprimer vos règles de translation.
Envoyer	Envoyer le fichier de configuration à l'IPS-Firewall NETASQ, et le programmer à l'heure d'activation spécifiée.
Annuler	Annuler les modifications depuis le dernier envoi à l'IPS-Firewall NETASQ et revenir à la liste des slots.

Une ligne est dite sélectionnée quand un de ses éléments est sélectionné (en inverse vidéo).

En plus de ces actions, vous pouvez utiliser pour chaque cellule du tableau les fonctionnalités de copier coller standard :

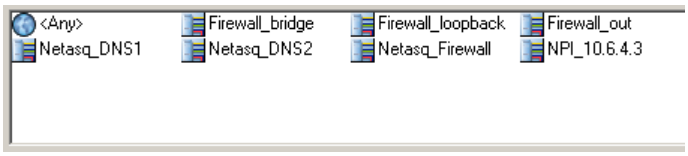
- ► Soit avec la souris (clic bouton droit),
- ► Soit avec les touches CTRL-C pour copier, CTRL-V pour coller,
- ► Soit avec les touches CTRL-Insert pour copier, Shift-Insert pour coller.

Menu contextuel



Le menu contextuel est activable par un clic droit sur une ligne sélectionnée dans la grille. Les différentes actions proposées sont des raccourcis aux boutons équivalents situés dans la barre d'outils.

Menu Drag & Drop



Comme son l'indique le menu « Drag'n Drop » permet en un Drag & Drop de positionner dans les règles de translation, les objets configurés dans le chapitre précédent. L'opération de Drag & Drop consiste à :

1. Sélectionner un objet,
2. Maintenir le bouton de souris enfoncé,
3. Réaliser un glissement de l'objet vers grille de règles,
4. Enfin y déposer l'objet.

Lorsque l'administrateur réalise une opération de Drag'n Drop, les champs disponibles pour l'objet sélectionné apparaissent en surbrillance.

Le menu de sélection des types d'objet situé à gauche du menu Drag'n Drop permet de sélectionner le type d'objet affiché dans la grille.

Affichage de la grille

L'affichage des données contenues dans la grille peut être défini suivant les préférences de l'administrateur parmi les options d'affichage : grandes icônes, petites icônes, détaillé ou en liste.

Options d'affichage

Deux options d'affichage des données de la grille du menu Drag'n Drop sont disponibles.

Montrer que les objets utilisés

Comme son nom l'indique, cette option permet d'afficher dans la grille que les objets qui sont actuellement utilisés dans les règles de translation.

Montrer les objets spéciaux

Les objets spéciaux sont les objets créés par défaut par l'IPS-Firewall et qui seront utilisés à l'activation des services associés (par exemple : Firewall_pptpXX, Firewall_dialupXX, Firewall_ipsec…). Ces objets rendent la lecture générale difficile et sont cachés par défaut.

Analyseur de cohérence et de conformité des règles

La politique de translation d'un IPS-Firewall est un des éléments les plus importants pour la sécurité des ressources que l'IPS-Firewall protège. Bien que cette politique évolue sans cesse, s'adapte aux nouveaux services, aux nouvelles menaces, aux nouvelles demandes des utilisateurs, elle doit conserver une cohérence parfaite afin que des failles n'apparaîssent pas dans la protection que propose l'IPS-Firewall.

L'enjeu est d'éviter la création de règles qui en inhiberait une autre. Lorsque la politique de translation est conséquente, le travail de l'adminstrateur est d'autant plus fastidieux que ce risque s'accroît. De plus lors de la configuration avancée de certaines règles de translation très spécifiques, la multiplication des options pourrait entraîner la création d'une règle erronée, ne correspondant plus aux besoins de l'administrateur.

Pour éviter ces écueils, l'écran d'édition des règles de translation des IPS-Firewalls dispose d'un analyseur de cohérence et de conformité des règles qui prévient l'administrateur en cas d'inhibition d'une règle par une autre ou d'erreur sur une des règles qui a été créées.

Divisé en deux onglets, cet analyseur regroupe les erreurs de création de règles dans l'onglet « Erreurs » et les erreurs de cohérence dans les règles dans l'onglet « Avertissements ».

Section B
Filtrage

© Copyright NETASQ 2006

Pour cette section, vous devez avoir franchi les étapes

► Installation, pré-configuration, intégration,
► Configuration réseau,
► Configuration des objets,
► Politique de translations.

Pour cette section, vous devez connaître

La politique de sécurité que vous voulez instaurer.

Utilité de la section

Cette section vous permet de définir les règles de filtrage. C'est le "cœur" de votre politique de sécurité.

Vous définissez ici qui utilise quoi, quand et comment.

Vous pouvez aussi bien limiter l'accès de l'intérieur vers l'extérieur et/ou la DMZ que de l'extérieur vers l'intérieur et/ou la DMZ...

Vous pouvez aussi définir les règles d'authentification pour vos utilisateurs : services ou machines nécessitant une authentification.

Introduction à cette section

La technologie ASQ inclut un moteur de filtrage dynamique des paquets (stateful inspection) avec optimisation des règles permettant l'application de la politique de filtrage de manière sûre et rapide. La mise en œuvre des fonctions de filtrage est basée sur la confrontation des attributs de chaque paquet IP reçu aux critères de chaque règle du slot de filtrage actif. Le filtrage porte sur tous les paquets sans exception. Les critères des règles de filtrage sont :

► l'interface de réception des paquets IP couverts par la règle,
► la ou les machines à l'origine des flux d 'information couverts par la règle,
► le ou les protocoles IP, les services TCP/UDP ou les types de messages ICMP des flux d'information couverts par la règle,
► la ou les machines destinataires des flux d 'information couverts par la règle,
► l'utilisateur ou le groupe d 'utilisateurs autorisés par la règle.

Les attributs des paquets IP qui sont confrontés aux quatre premiers critères cités sont évidemment extraits des en-têtes Ethernet, IP, ICMP, UDP ou TCP des trames. En ce qui concerne l'utilisateur ou le groupe d'utilisateurs autorisés par la règle, à partir du moment où un utilisateur s'est identifié et authentifié avec succès à partir d'une machine donnée, l'IPS-Firewall note ce fait et attribue le nom de login de cet utilisateur à tous les paquets IP présentant l'adresse de cette machine comme adresse IP source. En conséquence, les règles qui spécifient l'authentification des utilisateurs,

© Copyright NETASQ 2006

même sans préciser de contraintes sur les utilisateurs autorisés, ne peuvent s'appliquer qu'à des paquets IP émis d'une machine à partir de laquelle un utilisateur s'est préalablement authentifié. Chaque règle de filtrage peut spécifier une action de contrôle et une action de journalisation. Il y a quatre valeurs possibles pour l 'action de contrôle :

► passer : le paquet est accepté et n'est pas confronté aux règles suivantes,
► bloquer : le paquet est détruit silencieusement,
► réinitialiser : le paquet est détruit et un signal TCP RST (cas TCP) ou ICMP unreachable (cas UDP) est envoyé à l'émetteur,
► aucune : le paquet est confronté aux règles suivantes (sert à spécifier une action de journalisation uniquement).

Si aucune règle de filtrage n'est applicable au paquet, ou si les seules qui le sont ne spécifient « aucune » action de contrôle, le paquet est détruit silencieusement.

Il convient de noter qu'à proprement parler, pour un ensemble de paquets IP liés à un même échange au niveau transport (connexion TCP, pseudo-connexion UDP ou ICMP), l'IPS-Firewall ne confronte que le paquet initial de l'échange aux règles du slot de filtrage courant. À la réception de tout paquet IP, préalablement à l'application des règles du slot de filtrage courant, le paquet est comparé aux connexions / pseudo-connexions actuellement établies. Si les attributs et les paramètres du paquet correspondent aux critères et à l'état d'une de ces connexions / pseudo-connexions, il est autorisé à passer sans être soumis aux règles de filtrage. Ce mécanisme permet notamment de gérer les échanges bi-directionnels (notamment les connexions TCP) sans avoir à définir une règle de filtrage dans les deux sens de traversée de l'IPS-Firewall.

Des règles de filtrage implicites sont générées par l'IPS-Firewall en liaison avec la configuration d'autres fonctions de sécurité. Ce sont les règles correspondant à : l'administration à distance du IPS-Firewall, l'authentification des utilisateurs et l'établissement des VPN. Par ailleurs, des règles de filtrage dynamiques sont également générées pour les protocoles nécessitant des connexions filles.

À tout instant du fonctionnement d'un IPS-Firewall, il y a un slot de filtrage actif.

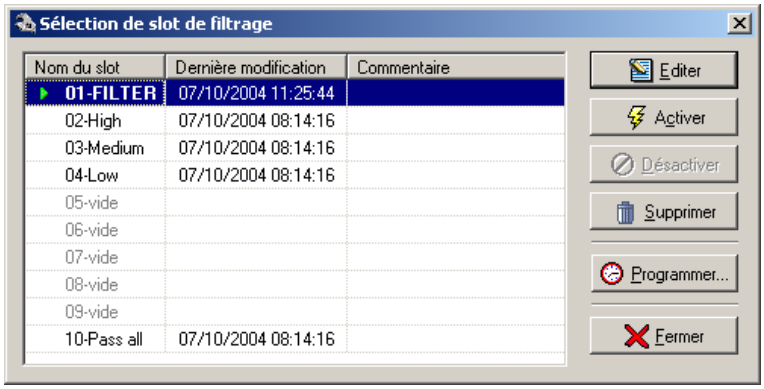
Les tables de filtrage sont stockées sur le Firewall NETASQ dans des slots (fichiers de configuration numérotés de 01 à 10). Chaque slot peut être programmé à une heure précise de la semaine, en écrasant la configuration du slot précédemment activé.

Le principe est simple : quand un paquet arrive au Firewall NETASQ (les règles de filtrage ne s'appliquant qu'en entrée d'interface, l'IPS-Firewall se fait confiance à lui-même pour les trafics qu'il génère comme par exemple RADIUS, LDAP, Kerberos, etc) , celui-ci fait descendre le paquet dans la liste de règles de filtrage. Si le paquet correspond aux critères de sélection d'une règle, il applique l'action associée à cette règle sinon le paquet est automatiquement supprimé. Une fois qu'une règle peut être appliquée au paquet, ce dernier n'est plus comparé aux règles suivantes.

La façon dont vos règles de filtrage sont ordonnées est primordiale. La cohérence de cet ordre est la principale difficulté dans la configuration de votre IPS-Firewall.

Accéder à cette section

Accédez à la boîte de dialogue par le sous-menu « Politique » - « Filtrage » de l'arborescence de l'interface graphique.



Lorsque vous sélectionner le sous menu « Politique > Filtrage » une boîte de dialogue s'affiche, elle vous permet de manipuler les slots associés au filtrage de paquets.

Elle est découpée en deux zones :

Gauche	Liste des slots.
Droite	Actions sur le slot sélectionné.

Liste des slots

Dans cette partie de la boite de dialogue se trouve la liste des slots. Il en existe 10, numérotés de 01 à 10.

Chaque slot possède un nom, une date/heure de mise en activité et la date de dernière modification effectuée sur ce slot. La programmation de l'activation de ces slots se fait grâce au programmateur horaire (Section D « programmation horaire »).

Le slot en cours d'activité est indiqué par une petite flèche verte à gauche de son nom. Un slot est dit " en activité " lorsque les paramètres qu'il contient sont en service. Il ne peut y avoir plus d'un slot en activité car les paramètres du dernier slot activé écrasent ceux du slot activé précédemment.

Si vous modifiez un slot, vous devez le réactiver pour prendre en compte les modifications. Un slot modifié mais non réactivé est notifié par l'icône à la place de la flèche verte habituelle.

Il y a toujours forcément un slot de filtrage actif.

Par défaut, un fichier de configuration contient une seule règle bloquant tous les paquets. Chaque slot ne doit pas obligatoirement contenir des paramètres.

Un slot pour lequel il n'existe pas de fichier de configuration sur le Firewall NETASQ est affiché sous le nom « vide » dans la liste.

Un slot est dit sélectionné quand vous faites un simple clic de la souris sur son nom. La sélection faite, vous pouvez l'éditer ou l'activer.

© Copyright NETASQ 2006

Actions sur le slot sélectionné

Quand un slot est sélectionné, vous pouvez réaliser différentes actions :

Editer	Modifier les règles de filtrage associées à ce slot.
Activer	Activer immédiatement un slot : les paramètres enregistrés dans ce slot écrasent les paramètres en vigueur.
Programmer	Donner l'heure et le ou les jours auxquels le fichier va s'activer automatiquement.
Effacer	Efface le slot et toutes ses informations.
Fermer	Retour à l'écran principal.

Il existe un slot pré-configuré, appelé « Pass_all ». Ce slot laisse passer l'ensemble du trafic IP en provenance et à destination de tout le monde. Il est utile pour des phases de tests. Son utilisation dans un autre cadre pourrait se révéler dangereux pour la sécurité de vos ressources sensibles.

Lorsque vous utilisez la translation d'adresses, ne créez pas de règles de filtrage pour les adresses IP virtuelles, utilisez toujours le nom d'objet réel.

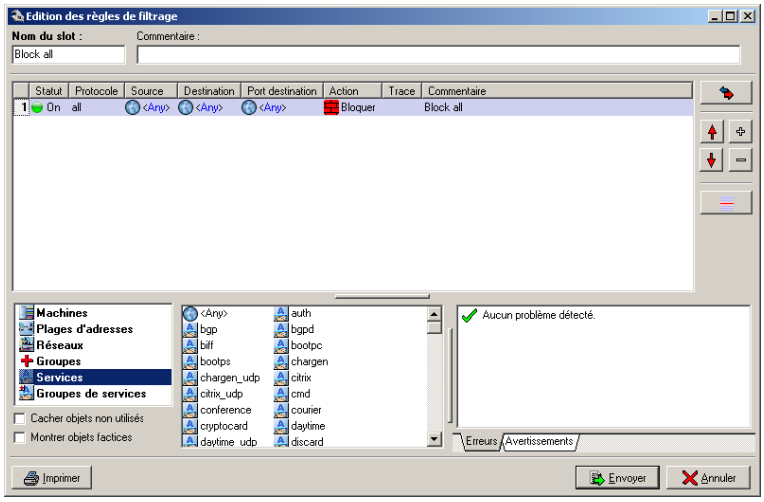
L'action « Bande Passante » (voir plus loin) vous permet de faire de la régulation de bande passante par service. Un calcul de dérivée de la courbe du trafic permet de déterminer si des paquets doivent être supprimés silencieusement afin de ne pas dépasser le débit limite. Pour les services utilisant TCP, la ré-émission des paquets supprimés sera gérée par TCP. Pour les services utilisant UDP, les paquets ne seront pas ré-émis.

© Copyright NETASQ 2006

Reportez-vous à la procédure suivante pour éditer un slot de filtrage :

1. Sélectionnez un slot dans la liste des slots de filtrage,

2. Cliquez sur le bouton « Editer » de la boite de dialogue contenant la liste des slots de filtrage.



La fenêtre d'édition d'un slot de filtrage apparaît. Elle est composée de plusieurs parties :

- ► Une zone comportant les règles de filtrage sous la forme d'un tableau ;
- ► Un menu Drag'n Drop ;
- ► Un analyseur de cohérence et conformité des règles ;
- ► Une zone d'actions possibles.

Règles de filtrage

Cette grille vous permet de définir les règles de filtrage à appliquer. Faites attention à bien ordonner vos règles de filtrage afin d'avoir un résultat cohérent. Le Firewall exécute les règles dans l'ordre d'apparition à l'écran et s'arrête dès qu'une action s'applique au flux qui tente de le traverser. Il convient donc de définir les règles dans l'ordre du plus détaillé au plus général.

Statut	Activation/désactivation d'une règle au sein d'un slot.
Protocole	Protocole sur lequel s'applique la règle de filtrage.
Source	Objet source utilisé comme critère de sélection pour cette règle. Un double clic sur cette zone permet de choisir l'objet associé. Le sélecteur d'objets n'affiche que les objets disponibles pour ce champ.
Destination	Objet destination utilisé comme critère de sélection pour cette règle. Un double clic sur cette zone permet de choisir l'objet associé. Le sélecteur d'objets n'affiche que les objets disponibles pour ce champ.
Port de destination	Service ou groupe de service utilisé comme critère de sélection

© Copyright NETASQ 2006

	pour cette règle. Un double clic sur cette zone permet de choisir l'objet associé. Le sélecteur d'objets n'affiche que les objets disponibles pour ce champ.
Action	Action appliquée sur le paquet remplissant les critères de sélection de cette règle de filtrage.
Traces	Type de trace générée.
Commentaire	Commentaires que vous voulez associer à cette règle.

Au niveau de la colonne « Statut », une lumière verte signifie que lors de l'activation du slot, cette règle sera appliquée, une lumière rouge signifie qu'elle ne sera pas appliquée. Ceci permet de définir des règles qui seront utilisées ultérieurement ou de désactiver temporairement certaines règles pour faire des tests.

Attention, par défaut les règles sont inactives (lumière rouge).

A la gauche des noms d'objets (source et destination) se trouve une icône d'état, indiquant la nature de l'objet (machine ou réseau). Le symbole « + » apparaît lorsqu'il s'agit d'un groupe d'objets.

A la gauche des services se trouve une icône d'état, représentant le type de service. De même, le symbole « + » apparaît pour signifier qu'il s'agit d'un groupe.

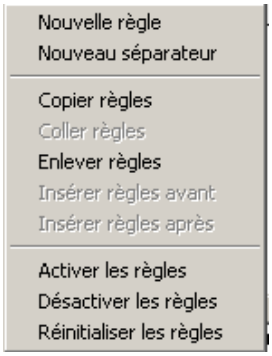
Si une règle n'est pas ou plus valide, elle passe automatiquement à l'état "OFF" et une icône avec un point d'exclamation apparaît dans la colonne posant problème.

Actions possibles sur les slots

Nom du slot	Nom donné au fichier de configuration.
Commentaire	Commentaire indicatif associé au slot de filtrage.
Mode avancé	Affichage des paramètres de configuration avancés du filtrage.
Insérer .	Insérer une ligne vierge après la ligne sélectionnée.
Effacer	Supprimer la ligne sélectionnée.
Flèche vers le haut	Placer la ligne sélectionnée avant la ligne directement au dessus.
Flèche vers le bas	Placer la ligne sélectionnée après la ligne directement en dessous.
Insérer un séparateur	Cette option permet d'insérer un séparateur au dessus de la ligne sélectionnée afin d'indiquer un commentaire sur une ligne de l'édition du filtrage. Pour définir un séparateur, il s'agit d'indiquer un commentaire et une couleur pour ce séparateur.
Imprimer	Impression de la configuration du filtrage.

Une ligne est sélectionnée quand l'un de ses éléments est sélectionné (en inverse vidéo).

Menu contextuel



Le menu contextuel est activable par un clic droit sur une ligne sélectionnée dans la grille. Les options de ce menu sont des raccourcis aux boutons équivalents situés dans la barre d'outils.

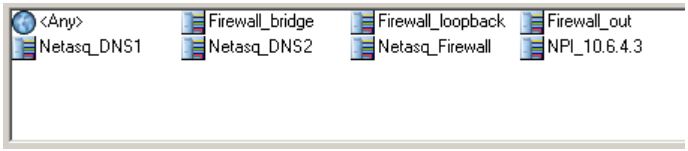
Vous pouvez accéder aux fonctionnalités du copier-coller grâce aux touches standards :

- ► CTRL-c pour copier, CTRL-v pour coller,
- ► CTRL-d pour supprimer la ligne,
- ► Ins pour insérer une ligne après la ligne en cours,
- ► Maj+Ins pour insérer une ligne avant la ligne en cours,

Vous pouvez supprimer une ligne en appuyant directement sur la touche « Suppr » du Clavier.

Vous pouvez déplacer une règle avec les touches + et - du clavier.

Menu Drag & Drop



Comme son nom l'indique le menu « Drag'n Drop » permet en un Drag & Drop de positionner les objets configurés dans le chapitre précédent dans les règles de filtrage. L'opération de Drag & Drop consiste à :

- ► Sélectionner un objet,
- ► Maintenir le bouton de souris enfoncé,
- ► Réaliser un glissement de l'objet vers la grille de règles,
- ► Enfin y déposer l'objet.

Lorsque l'administrateur réalise une opération de Drag'n Drop, les champs disponibles pour l'objet sélectionné apparaissent en surbrillance.

Le menu de sélection des types d'objet situé à gauche du menu Drag'n Drop permet de sélectionner le type d'objet affiché dans la grille.

Affichage de la grille

L'affichage des données contenues dans la grille peut être défini suivant les préférences de l'administrateur parmi les options d'affichage : grandes icônes, petites icônes, détaillé ou en liste.

Options d'affichage

Deux options d'affichage des données de la grille du menu Drag'n Drop sont disponibles.

Montrer que les objets utilisés

Comme son nom l'indique, cette option permet d'afficher dans la grille que les objets qui sont actuellement utilisés dans les règles de translation.

Montrer les objets spéciaux

Les objets spéciaux sont les objets créés par défaut par l'IPS-Firewall et qui seront utilisés à l'activation des services associés (par exemple : Firewall_pptpXX, Firewall_dialupXX, Firewall_ipsec…). Ces objets rendent la lecture générale difficile et sont cachés par défaut.

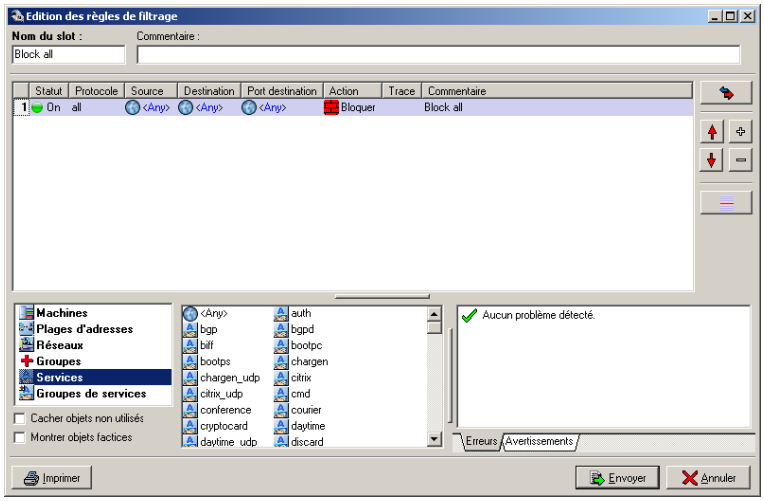
Analyseur de cohérence et de conformité des règles

La politique de filtrage d'un IPS-Firewall est un des éléments les plus importants pour la sécurité des ressources que l'IPS-Firewall protège. Bien que cette politique évolue sans cesse, s'adapte aux nouveaux services, aux nouvelles menaces, aux nouvelles demandes des utilisateurs, elle doit converser une cohérence parfaite afin que des failles n'apparaîssent pas dans la protection que propose l'IPS-Firewall.

L'enjeu est d'éviter la création de règles qui en inhiberait une autre. Lorsque la politique de filtrage est conséquente, le travail de l'adminstrateur est d'autant plus fastidieux que ce risque s'accroît. De plus lors de la configuration avancée de certaines règles de filtrage très spécifiques, la multiplication des options pourrait entraîner la création d'une règle erronée, ne correspondant plus aux besoins de l'administrateur.

Pour éviter ces écueils, l'écran d'édition des règles de filtrage des IPS-Firewalls dispose d'un analyseur de cohérence et de conformité des règles qui prévient l'administrateur en cas d'inhibition d'une règle par une autre ou d'erreur sur une des règles qui a été créées.

Divisé en deux onglets, cet analyseur regroupe les erreurs de création de règles dans l'onglet « Erreurs » et les erreurs de cohérence dans les règles dans l'onglet « Avertissements ».



Cette section détaille la création de vos règles de filtrage. L'ordre de ces règles est important car l'IPS-Firewall les parcourt du haut vers le bas et s'arrête dès qu'il trouve une règle correspondant au paquet IP (sauf s'il exécute uniquement une option). Les règles d'authentification doivent être configurées dans cette section. Ces règles permettent de limiter à certains utilisateurs l'accès à certains services ou certaines machines.

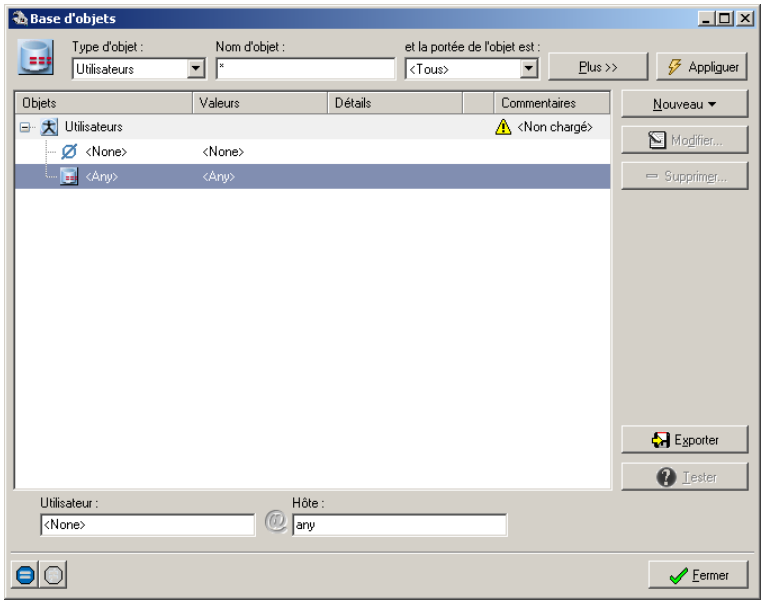
Activation et désactivation d'une règle

ON : La règle est utilisée pour le filtrage
OFF : La règle n'est pas utilisée pour le filtrage

L'activation et la désactivation d'une règle de filtrage facilitent la mise au point de vos filtres. Une règle désactivée n'est pas prise en compte par l'IPS-Firewall NETASQ lorsque le slot est activé.

Objet source et objet destination

© Copyright NETASQ 2006



Un double clic dans ces zones permet de choisir les objets concernés par la règle que vous voulez mettre en place, grâce à la boîte de dialogue de sélection des objets.

Choix de la source

Les sources des règles sont définies de la façon suivante : <User>@<IP>.

Pour préciser une source, vous devez donc choisir la partie <User> et la partie <IP>. La partie <User> peut être un utilisateur ou un groupe d'utilisateurs parmi ceux définis dans les objets du firewall. La partie <IP> peut être une machine, un groupe de machines, un réseau ou un groupe de réseaux définis dans les objets de l'IPS-Firewall.

Différents cas de figure rencontrés :

► <Any>@<Any> : la règle s'applique à toute machine mais nécessite une authentification de l'utilisateur,
► <No Auth>@<Any> : la règle s'applique à toute machine sans authentification,
► <No auth>@Object : la règle s'applique à l'objet "Object" (Object peut être une machine, un groupe de machines, un réseau ou un groupe de réseaux) et ne nécessite pas d'authentification,
► <Any>@Object : la règle s'applique à l'objet "Object" et nécessite une authentification de l'utilisateur,
► User@<Any> : la règle s'applique à toute machine à condition que l'utilisateur soit authentifié sous le login User,
► User@Object : la règle s'applique à l'objet "Object" et l'utilisateur doit être authentifié sous le login User.

Si une source possède une partie <user> différente de <No auth> alors une authentification sera nécessaire.

Choix de la destination

La destination est toujours une machine, un groupe de machines ou un réseau.

Remarques

L'objet « any » correspond à TOUTES LES adresses IP possibles. Il faut bien comprendre que l'objet « any » est un objet à part entière. Ce n'est pas un Joker qui remplace n'importe quel objet.

Les objets sont ceux que vous avez définis dans la section « Configuration des objets ».

Le champ vide sous les onglets vous permet de faire une recherche rapide dans la liste (avec la première lettre de l'objet par exemple).

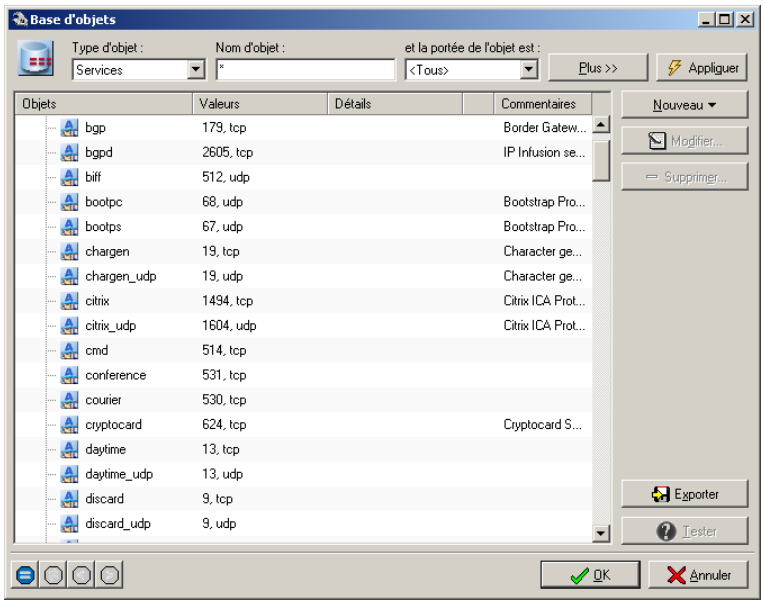
Sous les onglets, les boutons suivants apparaissent :

Opérateur	Signifie que l'objet concerné par la règle de filtrage est celui sélectionné. Signifie que l'objet concerné par la règle de filtrage est tout sauf celui sélectionné.
Editer	Permet de créer ou de supprimer des objets.
OK	Valide la sélection.
Annuler	Annule le choix et retourne à la fenêtre précédente.

L'objet source correspond toujours à l'initiateur de la communication.

Si vous utilisez la translation d'adresses, utilisez toujours comme Source l'objet « réel » (pas l'objet translaté) car le Firewall NETASQ applique les règles sur les adresses réelles.

Port de destination



Un double clic dans cette zone permet de choisir le service ou groupe de services concerné par la règle de filtrage, grâce à la boite de dialogue de sélection des services.

Vous pouvez choisir un service ou un groupe de services. Ces services sont ceux que vous avez définis dans la section « Configuration des objets ».

En bas de cette fenêtre, les boutons suivants apparaissent :

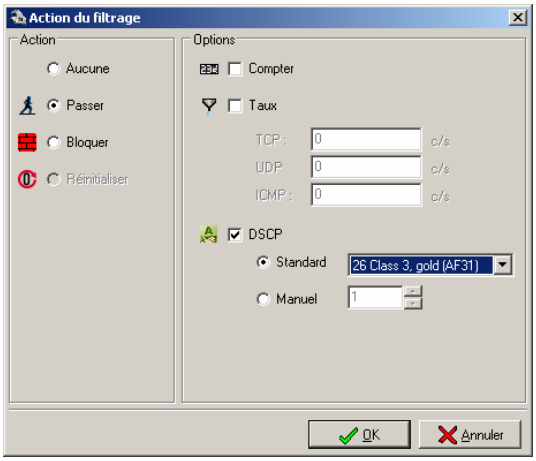
Opération	Signifie que le service concerné par la règle de filtrage est celui sélectionné. Signifie que les services concernés par la règle de filtrage sont tout sauf celui sélectionné. Signifie que tous les services concernés sont ceux dont le numéro de port est inférieur et égal au numéro de port du service

	sélectionné. Signifie que tous les services concernés sont ceux dont le numéro de port est supérieur et égal au numéro de port du service sélectionné.
Editer	Permet de créer ou de supprimer des objets.
OK	Valide la sélection.
Annuler	Annule le choix et retourne à la fenêtre précédente.

Le service correspond par défaut au port destination de la machine de destination. Les ports sources sont gérés automatiquement par le module « Stateful ».

Dans certains cas, vous pouvez avoir besoin de préciser les ports sources. Dans ce cas, il suffit de cliquer sur l'icône « Mode Avancé » située sous la grille de règles. Une colonne supplémentaire apparaît à côté de la colonne "Source". Elle est intitulée "Port Source". Vous pouvez, en double-cliquant sur cette colonne, choisir le service qui sera utilisé sur la machine source.

Actions



Un double clic dans cette zone permet de choisir l'action associée à la règle de filtrage, grâce à la boîte de dialogue de sélection des actions.

La partie gauche de l'écran contient l'ensemble des actions que vous pouvez effectuer :

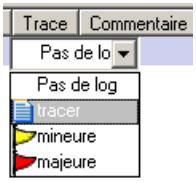
Aucun	L'IPS-Firewall NETASQ n'effectue aucune action. Ceci est utile si vous voulez juste tracer certains flux sans appliquer d'action particulière.
Passer	L'IPS-Firewall NETASQ laisse passer le paquet correspondant à cette règle de filtrage. Le paquet ne descend plus dans la liste de règles.
Bloquer	L'IPS-Firewall NETASQ bloque silencieusement le paquet correspondant à cette règle de filtrage : le paquet est supprimé sans que l'émetteur ne le sache. Le paquet ne descend plus dans la liste des règles.
Réinitialiser	L'IPS-Firewall NETASQ bloque explicitement le paquet correspondant à cette règle de filtrage : une réponse TCP/IP est envoyée par l'IPS-Firewall NETASQ à l'émetteur du paquet. Le paquet ne descend plus dans la liste des règles. Cette option n'est valable que pour certains services.

En complément de l'action « Passer », vous pouvez ajouter les options suivantes :

Compter	L'IPS-Firewall NETASQ compte le nombre de paquets correspondants à cette règle de filtrage et génère un rapport (dans les statistiques du compteur). Vous pouvez ainsi obtenir des informations de volumétrie sur les flux désirés.
Taux	L'IPS-Firewall NETASQ peut limiter le nombre maximal de connexions acceptées par seconde pour une règle de filtrage. Définissez, pour le protocole correspondant à la règle (TCP, UDP, ICMP), le nombre désiré. Attention, la limitation ne s'appliquera qu'à la règle correspondante : par exemple, si vous créez une règle HTTP, seule la limitation TCP sera prise en compte. Cette option vous permet aussi d'éviter le déni de service que pourrait tenter d'éventuels pirates : vous pouvez limiter le nombre de requêtes adressées à vos serveurs. *Remarque : si l'option est affectée à une règle contenant un groupe d'objets, la limitation s'applique au groupe dans son ensemble (nombre total de connexions).*
Bande passante	L'IPS-Firewall NETASQ vous permet de limiter la bande passante affectée à une règle de filtrage. Indiquez le nombre d'octets maximum accepté par seconde pour la règle associée. *Remarque : si l'option est affectée à une règle contenant un groupe d'objets, la bande passante accordée est donnée au groupe entier (total de la bande passante allouée pour tout le groupe).*
DSCP	Marquage du champ DSCP afin de définir une différenciation des flux. Le menu propose deux manières de définir le champs DSCP : selon les standards (la définition des classes fait l'objet d'une RFC) ou manuel (attention, cette option n'est pas compatible avec les équipements uniquement basés sur la qualification standard) Cette information peut être traitée par un équipement réalisant de la Qualité de Service (QoS). Cette option peut être associée au champ Service DSCP ou QoS de la configuration avancée du filtrage des IPS-Firewall NETASQ. Des exemples d'utilisation sont indiqués dans la section « DSCP et QoS » ci-dessous.

Certaines actions ou options ne sont disponibles qu'après avoir sélectionné le protocole ou service dans la règle de filtrage. Vous pouvez consulter les exemples de règles de filtrage en Annexe F pour une meilleure compréhension de ces choix.

Traces

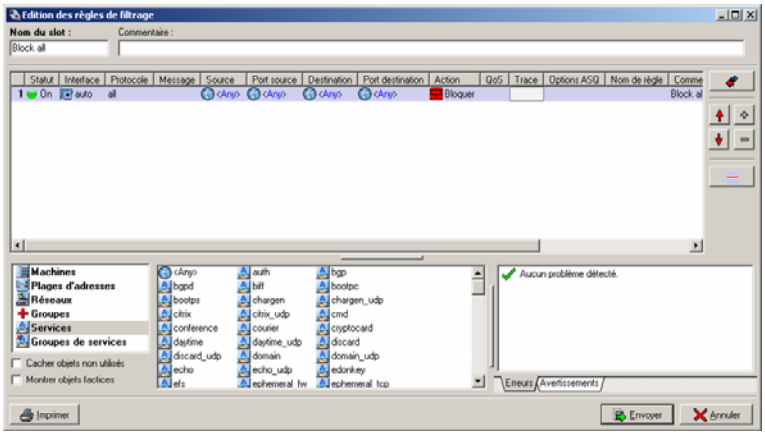


Un clic dans cette zone permet de définir la politique de traces pour la règle choisie.

Pas de log	Aucune action de traces n'est affectée à la règle.

Tracer	Dès que cette règle de filtrage est appliquée à une connexion, une trace est ajoutée dans les fichiers de traces, dans la partie filtrage.
Mineure	Dès que cette règle de filtrage est appliquée à une connexion, une alarme mineure est générée. Cette alarme est reportée dans les logs (partie alarmes), est envoyée au moniteur temps réel et peut être envoyée par email (voir Chapitre VIII Gestion des traces).
Majeure	Dès que cette règle de filtrage est appliquée à une connexion, une alarme majeure est générée. Cette alarme est reportée dans les logs (partie alarmes), est envoyée au moniteur temps réel et peut être envoyée par email (voir Chapitre VIII Gestion des traces).

Configuration avancée



En cliquant sur le bouton « Mode Avancé » en bas à gauche, de nouvelles colonnes apparaissent. Ceci vous permet de paramétrer d'autres champs relatifs à vos règles de filtrage :

Interface	La colonne interface permet de choisir l'interface sur laquelle doit s'appliquer la règle. Par défaut, le firewall la détecte automatiquement d'après l'adresse IP de la machine source (auto).
Service DSCP	DSCP pour Differentiated Services Code Point, permet comme son nom l'indique de déterminer grâce à un code préétabli, l'appartenance d'un trafic à un certain service plutôt qu'à un autre. Ce service DSCP, utilisé dans le cadre de la Qualité de Service, permet alors à l'administrateur d'appliquer des règles de QoS suivant la différenciation des services qu'il aura définis. Dans les règles de filtrage, lorsque l'administrateur spécifie un Service DSCP, il choisit de n'affecter la règle qu'aux trafics possédant le même DSCP. Ce champ peut être associé au champ QoS de la configuration avancée des règles de filtrage. Des exemples d'utilisation sont indiqués dans la section « DSCP et QoS » présente ci-dessous.
Message	Vous pouvez choisir les messages ICMP que vous désirez filtrer. La liste des messages ICMP est présentée en annexe.

Port Source	La colonne Port source permet de préciser le port utilisé par la machine source, si c'est une valeur particulière. Par défaut, le module Stateful mémorise le port source utilisé et seul celui-ci est autorisé pour les paquets retour.
QoS	Le champ QoS permet de définir la politique de Qualité de service associée au trafic. La configuration complète et l'utilisation de la QoS NETASQ sont indiquées dans le Chapitre IV Section E « Configuration de la QoS ».
Options ASQ	Trois options ASQ sont disponibles dans le champ des options ASQ. Le profil ASQ à appliquer au trafic. (Voir la « configuration ASQ »). Pas d'attachement automatique des plugins, pour désactiver l'attachement automatique des plugins pour cette règle de filtrage. Pas de signatures contextuelles, pour désactiver l'analyse par signatures contextuelles pour cette règle de filtrage.
Nom de la règle	Permet d'indiquer un nom à la règle de filtrage sélectionnée. Cette option est utile dans le cadre des tris dans le reporter.

Attention, ces options requièrent une très bonne connaissance du filtrage du firewall. Elles ne doivent être utilisées qu'en connaissance de cause.

Il n'est pas conseillé d'utiliser l'option de filtrage des messages ICMP sans une très bonne connaissance de la signification de ces derniers. L'option Filtrage des messages ICMP automatique (présente dans l'onglet « Analyse » du menu « Configuration > ASQ ») réalise déjà un filtrage ICMP en fonction du contexte des connexions.

DSCP et QoS

L'IPS-Firewall NETASQ fait partie intégrante de la politique de Qualité de Service devant être mise en place au sein d'une entreprise. En effet la plupart des flux stratégiques de cette Qualité de Service vont notamment transiter au travers de l'IPS-Firewall.

Ainsi l'administrateur d'un IPS-Firewall NETASQ doit pouvoir configurer l'ensemble des services que l'on peut attendre d'un équipement effectuant une Qualité de Service. Pour cela il dispose de trois options :

► **Le champ Service DSCP** : situé dans la configuration avancée du filtrage des IPS-Firewalls NETASQ, il permet la différenciation des trafics qui seront traités par le filtrage de l'IPS-Firewall.

► **L'action de réécriture du champ DSCP** : situé dans le menu de configuration de l'action associée à une règle de filtrage. Cette option permet tout simplement la modification du champ DSCP.

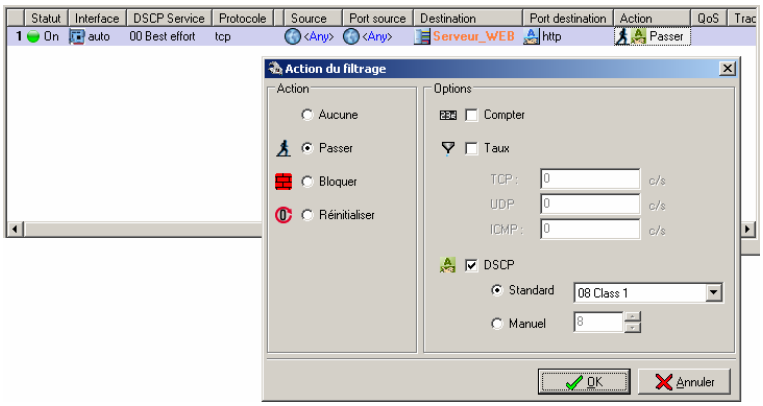
► **Le champ QoS** : situé dans la configuration avancée du filtrage des IPS-Firewalls NETASQ, cette option permet l'application de règles de QoS sur des trafics définis.

La combinaison de ces trois options permet la configuration complète d'une politique de QoS au niveau de l'IPS-Firewall.

Exemple 1 : Réécriture du champ DSCP

L'une des actions qui peut s'avérer très utile dans un premier temps est la réécriture du champ DSCP. Par exemple alors que sur Internet certains trafics ne sont pas différenciés, l'administrateur a mis en place une politique de QoS sur le réseau local qu'il souhaite pouvoir appliquer sur des trafics en provenance d'Internet. Dans ce cas, il est nécessaire de mettre en place un mécanisme de réécriture du champ DSCP qui marquera les trafics (jusqu'alors non différenciés) qui doivent être affectés par la politique de QoS.

La configuration de la politique de filtrage est alors la suivante :

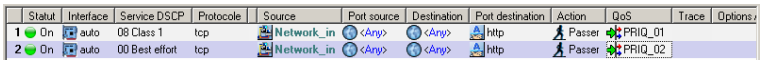


Ici, tous les trafics non différenciés à destination du serveur WEB voit leur champ DSCP réécrit.

Exemple 2 : Application d'une politique de QoS sur des trafics différenciés

L'autre utilisation principale des options de QoS expliquées plus haut est l'application d'une politique de QoS sur des trafics différenciés. En effet l'IPS-Firewall recevant des trafics différenciés grâce au champ « Service DSCP » peut alors appliquer la règle de QoS associée et définie par l'administrateur.

L'image suivante montre un exemple de configuration de la politique de filtrage :



Ici deux trafics quasiment identiques (trafic provenant du réseau local et à destination du WEB) sont traités différemment à cause du champ DSCP.

© Copyright NETASQ 2006

Section C

Programmation horaire

© Copyright NETASQ 2006

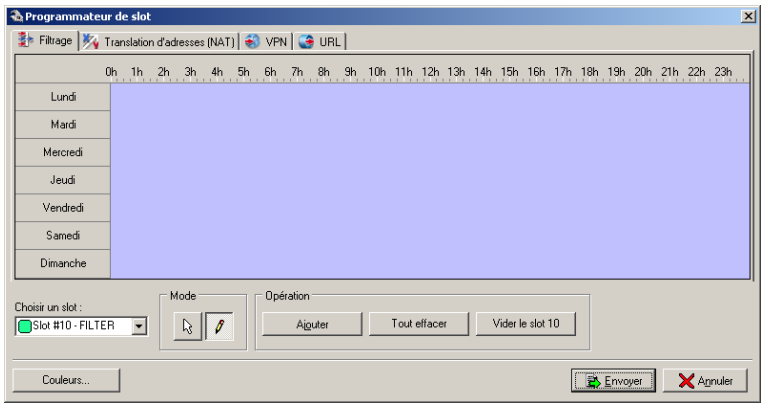
Les slots de filtrage et de chiffrement sont soumis à une programmation horaire. Pour chaque type de slot, l'administrateur possédant les droits « F+M » ou « V+M » (selon le type) utilise une grille horaire qui est construite comme un tableau interactif ; l'échelle horizontale représente les heures de la journée, et l'échelle verticale les jours de la semaine. En sélectionnant un des slots préalablement définis et en balayant avec la souris la surface correspondant à des plages horaires, on affecte ce slot à ces plages horaires.

Il doit toujours y avoir un slot de filtrage actif à un moment donné. Lorsque l'administrateur part d'une grille horaire de filtrage vierge pour définir ou modifier la programmation horaire du filtrage, le premier slot de filtrage que l'administrateur sélectionne est automatiquement affecté à toutes les heures de tous les jours de la semaine.

Vous pouvez configurer un slot pour qu'il ne s'active que lors des « heures de bureau », tout en programmant un blocage de tout trafic le reste du temps.

Pour programmer l'activation d'un slot vous avez deux possibilités :

- ► En sélectionnant le menu « Programmateur de slots »,
- ► En sélectionnant le bouton « programmer » présent dans chaque grille de slots.



La fenêtre de programmation horaire se décompose en trois parties :

- ► Des boutons de sélection de type de slots en haut,
- ► Une grille horaire,
- ► Des boutons d'action en bas.

Les boutons de sélection de type de slots

Quatre types de choix de slots sont disponibles.

Filtrage	Programmation des slots de filtrage.
Translation	Programmation des slots de translation d'adresses.
VPN	Programmation des slots de tunnels VPN.
Filtrage d'URL	Programmation des slots de filtrage d'URL.

La grille horaire

Cette zone est construite comme un tableau « interactif ». L'échelle horizontale représente les heures, l'échelle verticale : les jours. Grâce aux boutons d'action vous pouvez programmer l'activation des slots en sélectionnant une surface avec la souris.

© Copyright NETASQ 2006

On peut noter qu'au moins un slot de filtrage doit toujours être programmé. Donc lorsque vous programmez le premier de ces slots de filtrage celui-ci est automatiquement programmé pour tous les jours à toutes les heures.

Les boutons d'action

Choisir un slot	Sélection du slot à programmer.
Flèche	Sélection d'une zone sur la grille.
Crayon	Modification d'une zone sur la grille.
Gomme	Suppression d'une zone sur la grille.
Tout effacer	Suppression de toutes les zones sur la grille.
Vider le slot X	Suppression de toutes les zones concernant un slot.
Choisir les couleurs	Configuration des couleurs associées à chaque slot.

© Copyright NETASQ 2006

Chaque utilisateur est associé à un calendrier qui lui permet de s'authentifier auprès de l'IPS-Firewall lorsque la politique de filtrage instaurée par l'administrateur l'y oblige. Ce calendrier peut être spécifique à l'utilisateur ou le même pour plusieurs utilisateurs. Il définit les zones où l'utilisateur doit s'authentifier et celles où il n'a aucun accès. Une fois les calendriers définis, ils peuvent être sélectionnés lors de la configuration de l'authentification des utilisateurs. Vous accédez à la configuration de ce calendrier en sélectionnant le menu « Configuration > Calendriers ».

L'écran de sélection des calendriers se divise en trois parties :

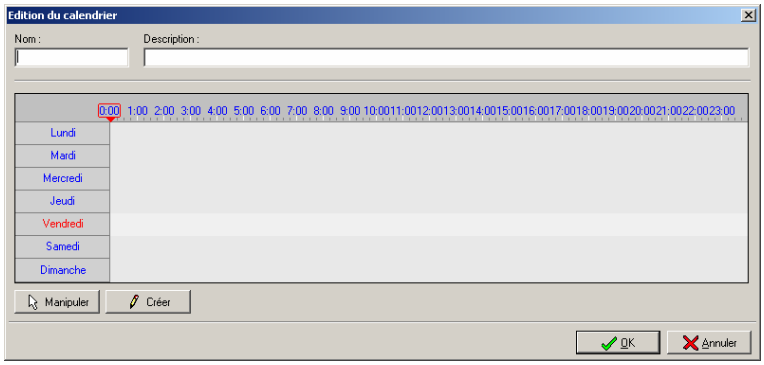
► Une grille contenant les calendriers configurés,
► Des boutons d'action permettant l'ajout, la modification ou la suppression de calendriers,
► Enfin en bas de la fenêtre les boutons de validation ou d'annulation des modifications effectuées.

Pour ajouter ou modifier un calendrier, vous avez plusieurs possibilités :

► En cliquant sur le bouton d'action « Calendrier » de l'onglet « Authentification » de l'écran d'édition d'un objet « utilisateur »,

► En cliquant sur le bouton d'action « Calendrier » du menu « Avancé » de l'écran de configuration générale de l'authentification, lorsque l'option « Autorisation par défaut » est à « Personnalisé »,

► En cliquant sur le bouton d'ajout ou de modification de l'écran de sélection des calendriers.



La fenêtre de configuration des calendriersse divise en deux parties :

► Le champ « Nom » : Nom défini pour le calendrier,
► Une grille horaire.

© Copyright NETASQ 2006

La grille horaire

Cette zone est construite comme un tableau « interactif ». L'échelle horizontale représente les heures, l'échelle verticale : les jours. Vous pouvez programmer les zones pendant lesquelles l'authentification est permise en sélectionnant une surface avec la souris. En cliquant sur les « titres » de colonnes et de lignes vous inversez la sélection actuelle dans la colonne ou dans la ligne en question. En cliquant le coin haut gauche de la grille vous inversez la sélection entière.

© Copyright NETASQ 2006

Section D

QoS : Qualité de Service

Qu’est ce que la Qualité de Service, QoS (pour Quality of Service) ?

Trois constats ont demandé le développement de la « Qualité de service » sur les réseaux IP :

► Premièrement de plus en plus les stations de travail modernes contiennent des logiciels multimédia y compris codecs vidéo et audio, cela nécessite donc une certaine fiabilité des performances (vitesse) vidéo.

► Le développement de plus en plus courant du multicast d’IP.

► Enfin le développement de logiciels vidéo et audio hautement performants permettant la vidéoconférence par exemple.

Ce type d’application en temps réel ne pouvait se révéler fonctionnel sur l’Internet étant donné les délais de latence et pertes de paquets généralement rencontrés sur les réseaux IP. Les développements de la « Qualité de service » se sont donc avérés indispensable.

A un haut niveau d’abstraction, la « Qualité de service » fait référence à la capacité à fournir un service réseau en fonction de paramètres définis dans un contrat de niveau de service (SLA, « Service Level Agreement »). La « Qualité » du service est alors caractérisée par sa disponibilité, son taux de latence, ses fluctuations, son débit et son taux de paquets perdus.

Au niveau des ressources réseau, la « Qualité de service » fait référence à la capacité d’un équipement à fournir des services de prioritisation de trafic, un contrôle de la bande passante ainsi que de son temps de latence.

QoS sur les IPS-Firewalls NETASQ

Le module Stateful QoS de l'ASQ permet une gestion efficace de la bande passante. Vous avez la possibilité d'associer une politique de QoS à chaque règle de filtrage en choisissant un algorithme d'ordonnoncement des paquets.

Deux algorithmes sont proposés : PRIQ (Priority Queuing) et CBQ (Class-Based Queuing).

► PRIQ permet de prioritiser les paquets associés à une régle de filtrage de façon qu'ils soient toujours traités en premier avant le reste du trafic ;

► CBQ permet de traiter les paquets par classe de bande passante. Vous avez la possibilité de choisir une classe d'ordonnoncement pour chaque régle de filtrage et de lui associer une garantie de bande passante aussi bien qu'une limite.

En cas d'utilisation simultanée de CBQ et PRIQ, les flux en PRIQ seront traités de façon prioritaire par rapport aux flux en CBQ.

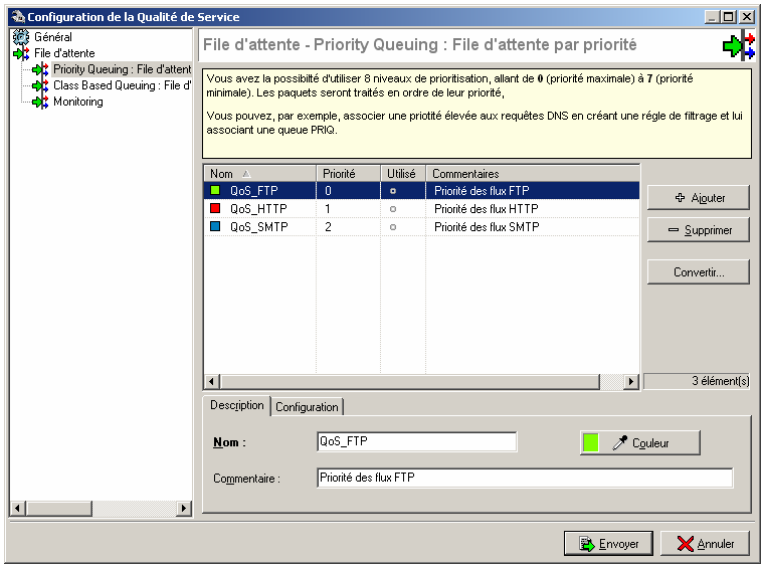
© Copyright NETASQ 2006

Menu de configuration de la QoS

La configuration de la QoS est accessible par le sous-menu « Qualité de Service » présente, sous le menu « Politique » de l'arborescence des menus de l'application Firewall Manager ou lors de l'édition d'une politique de filtrage, en cliquant sur le bouton « Configurer la QoS » accessible dans le menu « Paramétres de QoS de la règle de filtrage » obtenu lorsqu'on souhaite remplir le champ « Qos » d'une règle de filtrage (en mode avancé).

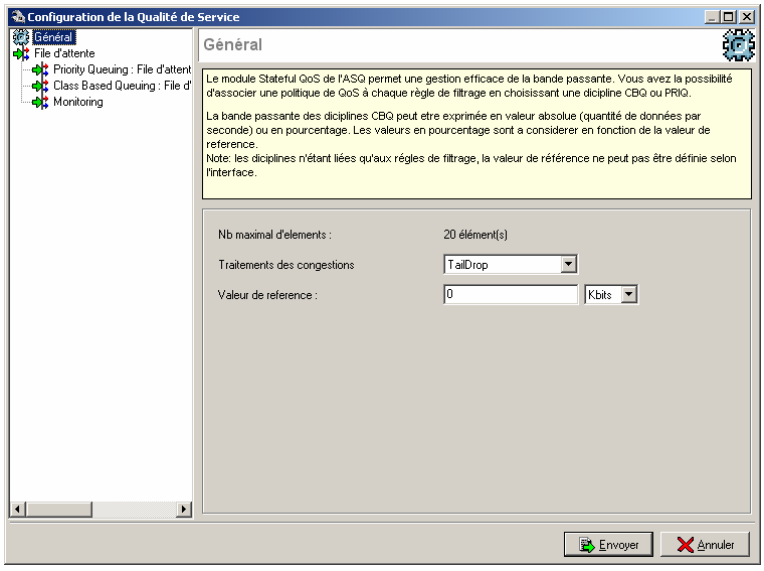
Le menu de configuration de la QoS est divisé en deux parties :

- A gauche un arbre présentant les diverses fonctionnalités du menu QoS,
- A droite les options configurables.



© Copyright NETASQ 2006

Général


Configuration de la Qualité de Service
Général
File d'attente
Priority Queuing : File d'attent
Class Based Queuing : File d'
Monitoring
Général
Le module Stateful QoS de l'ASQ permet une gestion efficace de la bande passante. Vous avez la possibilité d'associer une politique de QoS à chaque règle de filtrage en choisissant une dicipline CBQ ou PRIQ.
La bande passante des diciplines CBQ peut etre exprimée en valeur absolue (quantité de données par seconde) ou en pourcentage. Les valeurs en pourcentage sont a considerer en fonction de la valeur de reference.
Note: les diciplines n'étant liées qu'aux régles de filtrage, la valeur de référence ne peut pas être définie selon l'interface.
Nb maximal d'elements :
20 élément(s)
Traitements des congestions
TailDrop
Valeur de reference :
0
Kbits
Envoyer
Annuler

Les différentes options de la configuration générale sont présentées dans le tableau suivant :

Nb maximal d'éléments	Donnée indicative présentée par le Firewall Manager, dépendante du modèle de l'IPS-Firewall (20 pour les F25 et F50, 100 pour les F200 et F500, 200 pour les F1000 et F2000, 255 pour le F5000,indicant le nombre de file d'attente qui peuvent être créées.
Traitement des congestions	Cette option permet de définir l'algorithme de traitements des congestions qui sera utilisé lorsque le IPS-Firewall n'est plus à même de gérer tout le trafic qu'il reçoit.
Valeur de référence	La valeur de référence en Kbits/s ou en Mbits/s permet d'indiquer une référence sur laquelle seront basées les limitations de bande passante indiquée en pourcentage dans la configuration des files d'attente.

Traitements des congestions

Un élément important dans la « Qualité de Service » est de résoudre le problème du niveau généralement très haut du taux de perte de paquets sur l'Internet. En effet lorsqu'un paquet est perdu avant d'atteindre sa destination toutes les ressources mises en œuvre lors de son transit sont gâchées. Dans certain cas, cette situation peut même amener une situation de congestion grave qui parfois entraîne la paralysie totale des systèmes.

On est loin de la nécessité de stabilité et de « temps réel » des applications de vidéoconférence d'aujourd'hui. Le contrôle optimisé des situations de congestion et la gestion des queues de données deviennent un enjeu important de la « Qualité de Service ».

Les IPS-Firewalls NETASQ disposent de deux algorithmes pour leur traitement des congestions, l'algorithme TailDrop et l'algorithme BLUE. NETASQ recommande toutefois l'utilisation de l'agorithme BLUE comme algorithme de traitement des congestions.

TailDrop

Le principe de cet algorithme très basique est de supprimer les paquets arrivant dans la file d'attente lorsque celle-ci est pleine.

Blue

Cet algorithme très performant (de très loin devant la plupart des autres algorithmes) utilise un historique des paquets perdus et le taux d'utilisation des interfaces réseau pour gérer leur congestion.

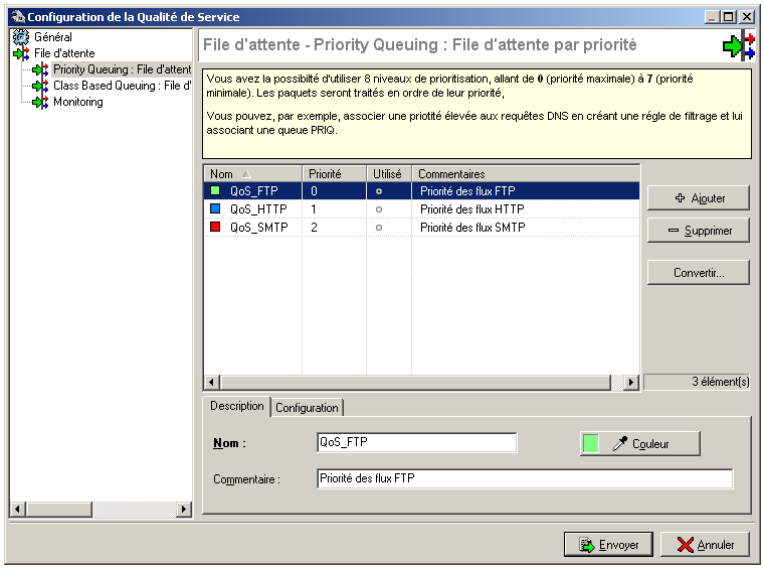
Le principe général de cet algorithme est de définir une probabilité unique (P) qui est ensuite utilisée pour marquer (par l'option de congestion de trafic ECN) ou pour dropper des paquets de la file de données. Le taux de perte de paquets en file fait augmenter cette probabilité (P). Par exemple, dans le cas d'un débordement de tampon (Buffer Overflow), la file de données perd continuellement des paquets de la file, la probabilité (P) est incrémentée, ce qui a pour effet d'augmenter artificiellement le nombre de paquets marqués (par ECN) ou le nombre de paquets droppés. Inversement lorsque le taux d'utilisation de l'interface réseau est faible voire nul, la probabilité (P) est alors diminuée.

Cette méthode a pour effet de stabiliser les flux réseaux, de réduire fortement le nombre de paquets finalement perdus, de maximiser les performances de chaque interface réseau et enfin de diminuer le temps de latence des paquets (on rappelle que ces critères sont fondamentaux pour la SLA, « Service Level Agreement »).

Files d'attente

Le module de QoS, intégré à l'ASQ est associé au module de filtrage pour offrir les fonctionnalités de Qualité de Service. A l'arrivée d'un paquet, celui-ci est traité par une règle de filtrage puis l'ASQ affecte le paquet à la bonne file d'attente suivant la configuration du champ QoS de cette règle de filtrage. Il existe trois types de file d'attente sur le IPS-Firewalls. Deux sont directement associés aux algorithmes de QoS présentés ci- dessus : PRIQ (Priority Queuing) et CBQ (Class-Based Queuing), le troisième type permet le monitoring du trafic.

Priority Queuing : File d'attente par priorité



Les files d'attente par priorité induisent une prioritisation des paquets dans leur traitement. Les paquets qui sont associés à une règle de filtrage avec une File d'attente du type PRIQ sont traités avant les autres.

Les priorités s'échelonnent entre 0 et 7. La priorité 0 correspond aux trafics les plus prioritaires parmi les files d'attente PRIQ. La priorité 7 correspond aux trafics les moins prioritaires parmi les files d'attente PRIQ. Les files d'attente CBQ et les flux sans règles de QoS sont associés à une priorité 8 « virtuelle » (elle n'est pas configurable) qui définit que quoi qu'il arrive, ces flux seront traités après toutes files d'attente du type PRIQ.

Les différentes options de la configuration d'une file d'attente du type PRIQ sont présentées dans le tableau suivant :

Ajouter	La grille du menu Priority Queuing affiche les différentes files d'attente qui ont été configurées. Le bouton « Ajouter » permet l'ajout d'une nouvelle file d'attente.
Supprimer	La grille du menu Priority Queuing affiche les différentes files d'attente qui ont été configurées. Le bouton « Supprimer » permet de supprimer la file d'attente sélectionnée.
Convertir	La conversion d'une file d'attente PRIQ en un autre type de file d'attente conserve le nom de la file d'attente et son commentaire.
xx élement(s)	Donnée cumulée présentée par le Firewall Manager indiquant le nombre de règles de QoS du type PRIQ qui ont été créées. Si le nombre total de règles de QoS (PRIQ, CBQ et Monitoring) est supérieur à la capacité maximum de gestion de l'IPS-Firewall indiquée dans le menu Général, un message apparaît en bas à gauche de l'écran pour indiquer que le nombre maximum de règle de QoS a été dépassé.

Onglet Description

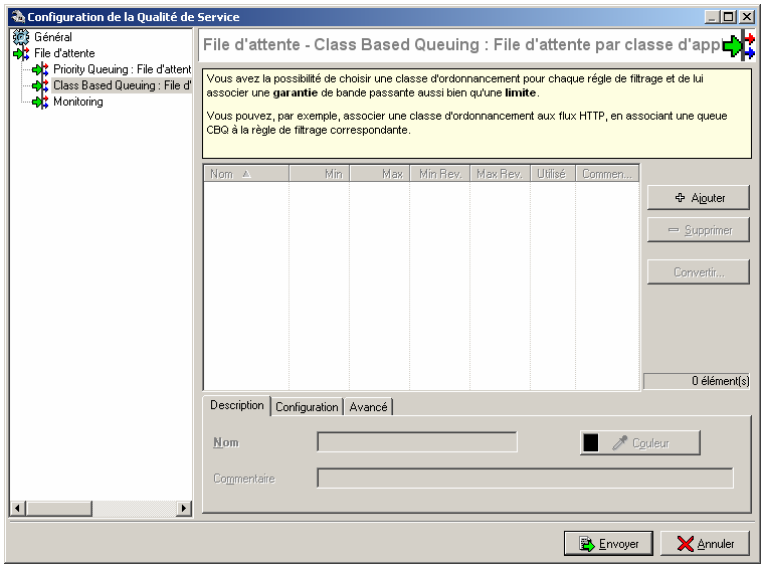
Nom	Nom de la file d'attente à configurer.
Commentaire	Commentaire associé.
Couleur	Couleur de différenciation de la file d'attente.

Onglet Configuration

Priorité	Priorité de la file d'attente configurée.

La grille du menu Priority Queuing affiche les différentes files d'attente qui ont été configurées. Lorsque ces règles de QoS sont effectivement utilisées dans la définition d'une règle de filtrage un bouton du type « » est affiché dans la liste. Un double clic sur le bouton permet d'affiche la liste des règles de filtrage dans lesquelles cette file d'attente est utilisée.

Class-Based Queuing : File d'attente par classe d'application ou d'affectation



Les files d'attente par classe d'application ou d'affectation induisent la façon dont les trafics affectés par ces règles de QoS seront gérés sur le réseau. Les mécanismes de réservation et de limitation de la bande passante de ce type de files d'attente permettent dans le premier cas, la garantie d'un service minimum et dans le deuxième cas, la préservation de la bande passante vis-à-vis d'applications coûteuses en ressources.

Les différentes options de la configuration d'une file d'attente du type CBQ sont présentées dans le tableau suivant :

Ajouter	La grille du menu Class-Based Queuing affiche les différentes files d'attente qui ont été configurées. Le bouton « Ajouter » permet l'ajout d'une nouvelle file d'attente.
Supprimer	La grille du menu Class-Based Queuing affiche les différentes files d'attente qui ont été configurées. Le bouton « Supprimer » permet de supprimer la file d'attente sélectionnée.
Convertir	La conversion d'une file d'attente CBQ en un autre type de file d'attente conserve le nom de la file d'attente et son commentaire.
xx élement(s)	Donnée cumulée présentée par le Firewall Manager indiquant le nombre de règles de QoS du type CBQ qui ont été créées. Si le nombre total de règles de QoS (PRIQ, CBQ et Monitoring) est supérieur à la capacité maximum de gestion de l'IPS-Firewall indiquée dans le menu Général, un message apparaît en bas à gauche de l'écran pour indiquer que le nombre maximum de règle de QoS a été dépassé.

Onglet Description

Nom	Nom de la file d'attente à configurer.
Commentaire	Commentaire associé.
Couleur	Couleur de différenciation de la file d'attente.

Onglet Configuration

L'onglet Configuration permet la définition des paramètres de réservation et de limitation de la bande passante pour cette file d'attente. La configuration de ces paramètres peut être asymétrique, ce qui signifie que les paramètres de réservation et de limitation seront différents suivant le sens du trafic.

Par défaut l'onglet Configuration définit les réservations et limitation de la bande passante dans les deux sens. Mais lorsque des paramètres sont indiqués dans l'onglet Avancé (voir ci-dessous), l'onglet Configuration définit les paramètres des trafics allant dans le sens de la défintion de la règle de filtrage soit « Source » vers « Destination ».

Maximum autorisé	Agissant comme une limitation, cette option interdit le dépassement de bande passante pour le trafic affecté par ces files d'attente. Configurée en Kbits/s, en Mbits/s ou en pourcentage de la valeur de référence, cette valeur est partagée entre tous les trafics affectés par la règle de QoS. Ainsi si les trafics HTTP et FTP sont associées à une file d'attente qui possède un maximum autorisé de 512Kbits/s alors la bande passante HTTP + la bande passante FTP ne doit pas dépasser 512Kbits/s.
Minimum garanti	Agissant comme une garantie de service, cette option permet la garantie d'un débit donné et d'un délai maximal de transfert. Configurée en Kbits/s, en Mbits/s ou en pourcentage de la valeur de référence, cette valeur est partagée entre tous les trafics

	affectés par la règle de QoS. Ainsi si les trafics HTTP et FTP sont associées à une file d'attente qui possède un minimum garanti de 10Kbits/s alors la bande passante HTTP + la bande passante FTP sera au minimum de 10Kbits/s. Cependant rien n'empêche que la bande passante HTTP soit de 9Kbits/s et la bande passante soit seulement de 1Kbit/s.
Pas de limite de bande passante	Cette option permet de ne pas définir de débit maximum autorisé. Dans ce cas c'est la valeur de la bande passante du lien affecté par la règle de QoS qui détermine le maximum disponible.

La grille du menu Class-Based Queuing affiche les différentes files d'attente qui ont été configurées. Lorsque ces règles de QoS sont effectivement utilisées dans la définition d'une règle de filtrage un bouton du type « » est affiché dans la liste. Un double clic sur le bouton permet d'affiche la liste des règles de filtrage dans lesquelles cette file d'attente est utilisée.

Onglet Avancé

L'onglet Avancé permet la configuration des paramètres de réservations et limitation de la bande passante des trafics allant dans le sens inverse de la défintion de la règle de filtrage soit « Destination » vers « Source ».

Maximum autorisé	Agissant comme une limitation, cette option interdit le dépassement de bande passante pour le trafic affecté par ces files d'attente. Configurée en Kbits/s, en Mbits/s ou en pourcentage de la valeur de référence, cette valeur est partagée entre tous les trafics affectés par la règle de QoS. Ainsi si les trafics HTTP et FTP sont associées à une file d'attente qui possède un maximum autorisé de 512Kbits/s alors la bande passante HTTP + la bande passante FTP ne doit pas dépasser 512Kbits/s.
Minimum garanti	Agissant comme une garantie de service, cette option permet la garantie d'un débit donné et d'un délai maximal de transfert. Configurée en Kbits/s, en Mbits/s ou en pourcentage de la valeur de référence, cette valeur est partagée entre tous les trafics affectés par la règle de QoS. Ainsi si les trafics HTTP et FTP sont associées à une file d'attente qui possède un minimum garanti de 10Kbits/s alors la bande passante HTTP + la bande passante FTP sera au minimum de 10Kbits/s. Cependant rien n'empêche que la bande passante HTTP soit de 9Kbits/s et la bande passante soit seulement de 1Kbit/s.
Pas de limite de bande passante	Cette option permet de ne pas définir de débit maximum autorisé. Dans ce cas c'est la valeur de la bande passante du lien affecté par la règle de QoS qui détermine le maximum disponible.

La grille du menu Class-Based Queuing affiche les différentes files d'attente qui ont été configurées. Lorsque ces règles de QoS sont effectivement utilisées dans la définition d'une règle de filtrage un bouton du type « » est affiché dans la liste. Un double clic sur le bouton permet d'affiche la liste des règles de filtrage dans lesquelles cette file d'attente est utilisée.

Monitoring

Les files d'attente de monitoring n'affectent pas la manière dont sont traités les trafics qui sont associés à ces règles de QoS. Elles permettent l'enregistrement d'informations de débit et de bande passante qui peuvent être visualisées au moyen du Firewall Reporter, dans la section « Graphique » du logiciel.

Les différentes options de la configuration d'une file d'attente du type Monitoring sont présentées dans le tableau suivant :

Ajouter	La grille du menu Monitoring affiche les différentes files d'attente

	qui ont été configurées. Le bouton « Ajouter » permet l'ajout d'une nouvelle file d'attente.
Supprimer	La grille du menu Monitoring affiche les différentes files d'attente qui ont été configurées. Le bouton « Supprimer » permet de supprimer la file d'attente sélectionnée.
Convertir	La conversion d'une file d'attente Monitoring en un autre type de file d'attente conserve le nom de la file d'attente et son commentaire.
xx élement(s)	Donnée cumulée présentée par le Firewall Manager indiquant le nombre de règles de QoS du type Monitoring qui ont été créées. Si le nombre total de règles de QoS (PRIQ, CBQ et Monitoring) est supérieur à la capacité maximum de gestion de l'IPS-Firewall indiquée dans le menu Général, un message apparaît en bas à gauche de l'écran pour indiquer que le nombre maximum de règle de QoS a été dépassé.

Onglet Description

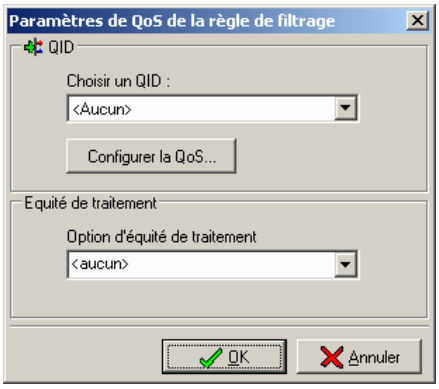
Nom	Nom de la file d'attente à configurer.
Commentaire	Commentaire associé.
Couleur	Couleur de différenciation de la file d'attente.

Activation d'une File d'attente de QoS

C'est dans la configuration des politiques de filtrage que sont définies les règles de QoS qui seront utilisées pour traiter tel ou tel trafic. Le champ correspondant à la QoS n'est accessible qu'une fois le mode avancé de la définition des règles de filtrage activé.

Pour activer une file d'attente de QoS, reportez-vous à la procédure suivante :

1. Sélectionnez le menu de configuration « Politique\Filtrage » ;
2. Editez le slot de filtrage dont les règles doivent accueillir les options de QoS ;
3. Sélectionnez le mode « Avancé » ;
4. Double cliquez sur le champ « QoS » de la règle à modifier, la fenêtre suivante apparaît :



5. Choisissez une File d'attente configurée (ou configurez la d'abord) ;
6. Choisissez l'équité de traitement (si nécessaire, voir ci-dessous) ;
7. Cliquez sur OK, envoyez le slot configuré et activez la politique de filtrage.

Equité de traitement (Fairness)

ATTENTION : l'équité de traitement complexifie la gestion de la QoS telle qu'elle a déjà été évoquée dans cette documentation. Assurez-vous de maîtriser les aspects précédents de la configuration de la QoS avant d'activer cette option.

L'équité de traitement (Fairness) ajoute à chaque file d'attente QoS un système de pondération des paquets propre à chaque file. Ainsi il est possible de modifier le comportement du traitement des paquets appartenant à la même file d'attente.

Selon l'option Fairness NETASQ, les paquets appartenant à une même file d'attente seront traités :

► Par ordre d'arrivée, selon le mode FIFO (First In First Out, premier arrivé, premier parti) si AUCUNE option d'équité de traitement n'a été spécifié ;

► De façon à ce que le traitement soit équitable (égal) entre les paquets de chaque utilisateur présents dans la file d'attente si l'option d'équité de traitement est UTILISATEUR ;

► De façon à ce que le traitement soit équitable (égal) entre les paquets de chaque machine présents dans la file d'attente si l'option d'équité de traitement est MACHINE ;

► De façon à ce que le traitement soit équitable (égal) entre les paquets de chaque connexion présents dans la file d'attente si l'option d'équité de traitement est CONNEXION.

© Copyright NETASQ 2006

Cas d'application et recommandations d'utilisation

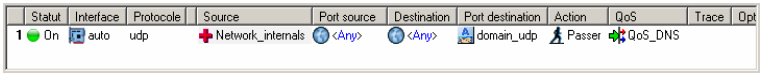
Exemple 1 : Prioritisation des flux DNS

Basées sur UDP, les requêtes DNS subissent de nombreuses pertes de paquets du fait de la définition même du protocole UDP, qui ne prévoit pas de mécanismes de gestion des erreurs de transmission et de l'écrasante présence des trafics TCP qui noient les trafics UDP dans la masse des paquets TCP.

Pour préserver ces trafics, et en particulier les flux DNS, il est recommandé de prévoir une règle de QoS de type « priorité » (PRIQ). Elle permettra de diminuer les trop fréquentes pertes de paquets et la latence qu'il pourrait y avoir sur ce type de trafic qui demande une réactivité importante (c'est d'ailleurs pour cette raison que les requêtes DNS sont réalisées sur UDP).

Définition de la règle de QoS pour le DNS

Utilisation de la règle de QoS dans la politique de filtrage



Effets sur le trafic

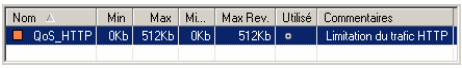
- ► Baisse des paquets perdus ;
- ► Diminution de la latence.

Exemple 2 : Limitation du trafic HTTP

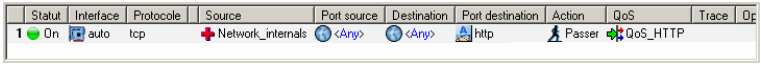
Parmi les trafics internet, les flux HTTP sont les plus gros consommateurs de la bande passante du lien Internet et du réseau local. Une utilisation importante de l'internet peut entraîner des problèmes de congestions du trafic réseau, les performances globales sont dégradées et l'utilisation du réseau devient fastidieuse.

Pour remédier à cet état de fait, il est recommandé de **limiter le trafic HTTP au moyen d'une règle de QoS de type « classe d'application ou d'affectation » (CBQ) définissant un débit maximum autorisé**. Elle permettra de préserver la bande passante du réseau et réduire l'impact de l'utilisation de l'internet sur les performances globales du réseau.

Définition de la règle de QoS pour le HTTP



Utilisation de la règle de QoS dans la politique de filtrage



Effets sur le trafic

- ► Diminution du risque de congestion du réseau ;
- ► Réduction de l'impact du trafic sur les performances générales du réseau.

Exemple 3 : Garantie d'un niveau de service minimum

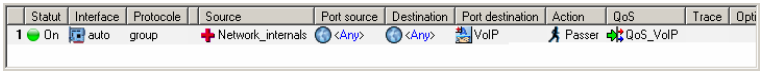
Certaines applications (VoIP par exemple) nécessitent un niveau de services avec la garantie que ce niveau de services sera respecté sous peine de dysfonctionnement du service (impossiblité de suivre une conversation VoIP par exemple). Les autres applications et leur impact sur les performances générales du réseau peuvent perturber l'obtention du niveau de services requis.

© Copyright NETASQ 2006

Pour s'assurer que le niveau de services requis sera maintenu il est recommandé de créer une règle de QoS de type « classe d'application ou d'affectation » (CBQ) définissant un débit minimum garanti. Elle permettra de garantir un niveau de service pour un trafic donné indépendamment de l'impact des autres trafics sur les performances globales du réseau et sans définir de limitation de bande passante pour ces autres trafics.

Définition de la règle de QoS pour la VoIP

Utilisation de la règle de QoS dans la politique de filtrage



Effets sur le trafic

- ► Garantie d'un niveau de service pour un trafic donné ;
- ► Introduction d'un délai maximal de transfert des données du service.

© Copyright NETASQ 2006

Chapitre V
VPN

Qu'est ce que le VPN ?

Les Réseaux Privés Virtuels ou RPV (VPN : Virtual Private Network, dans la littérature anglaise) permettent la transmission sûre de données sensibles au travers d'un média non sûr tel que peut l'être l'Internet. Cette transmission sûre est assurée par des mécanismes de chiffrement et d'authentification de l'ensemble de la communication entre ce que l'on appelle les correspondants VPN.

Technologies VPN intégrées sur l'IPS-Firewall

Les IPS-Firewalls NETASQ possèdent trois technologies pour assurer ses fonctionnalités VPN. Ces trois technologies correspondent à une utilisation spécifique du VPN :

► IPSEC : protocole standard, l'IPSEC permet la création de tunnels VPN entre l'IPS-Firewall et un autre firewall ou entre l'IPS-Firewall et des nomades sur lesquels seraient installés des clients VPN.

► PPTP : protocole propriétaire Microsoft, permet la création de tunnels VPN entre l'IPS-Firewall et des nomades sur lesquels existent un client PPTP intégré.

► SSL : cette dernière technologie permet la création de tunnels VPN entre l'IPS-Firewall et des nomades. Mais contrairement au deux autres technologies, la technologie SSL permet la création de tunnels VPN sans nécessiter l'installation de client VPN sur la machine nomade.

Organisation de la section VPN

Pour faciliter la compréhension des fonctionnalités VPN et de leur technologie associée, la section VPN se divise en trois parties (bien que la partie IPSEC soit la plus importante) qui contiennent chacune une introduction à la technologie associée, sa configuration sur l'IPS-Firewall et enfin des exemples de configuration.

© Copyright NETASQ 2006

Section A
IPSEC

© Copyright NETASQ 2006

Caractéristiques principales d'IPSEC

Le terme IPSEC (IP Security) désigne un ensemble de mécanismes de sécurité destiné à garantir une sécurité de haute qualité, basée sur la cryptographie, sans problème d'interopérabilité, pour le trafic au niveau d'IP (IPv4, IPv6). Les services proposés par IPSEC offre le contrôle d'accès, l'intégrité en mode non connecté, l'authentification de l'origine des données, la protection contre le rejeu, la confidentialité (chiffrement), et une certaine confidentialité sur le flux de trafic. Ces services sont offerts par IP ou par d'autres protocoles de couches supérieures. Ainsi IPSEC est indépendant des technologies de la couche Liaison de données ((ATM, Frame Relay, Ethernet,...).

IPSEC utilise deux protocoles pour assurer la sécurité du trafic : « Authentication Header (AH) » et « Encapsulating Security Payload (ESP) ». Ces protocoles ont également été conçus pour être indépendants de tout algorithme. Cette modularité permet de sélectionner différents types d'algorithme sans affecter la partie implémentation. Par exemple, des communautés différentes d'utilisateurs peuvent sélectionner (ou même créer) différents types d'algorithmes si nécessaire.

Chacun des protocoles ci-dessus supporte deux modes d'utilisation : le mode transport et le mode tunnel. En mode transport, le protocole propose une protection préliminaire pour les protocoles supérieurs à IP, et en mode tunnel, le protocole est utilisé dans les paquets IP envoyés en tunneling (sécurisation de la couche transport et de la couche IP).

Basé sur la cryptographie, un certain nombre de paramètres de communication doivent être négociés préalablement à l'échange d'information. Ce contexte (algorithmes de chiffrement, clefs, mécanismes sélectionnés…) est réuni au sein d'une SA (Security Association). Le concept de SA fait partie intégrante d'PSEC.

L'IPSEC natif ne supporte pas la translation d'adresses. IPSEC ne permet pas d'établir un tunnel VPN si au moins une des deux extrémités du tunnel possède une adresse translatée (cf Support de la fonctionnalité NAT-T).

Deux protocoles pour la sécurité du trafic

Authentication Header (AH)

L'entête d'authentification AH (Authentication Header) a été conçu pour assurer l'intégrité en mode non connecté, l'authentification de l'origine des données, et un service anti-rejeu optionnel. Le principe d'AH est d'adjoindre au datagramme IP classique un champ supplémentaire permettant à la réception de vérifier l'authenticité des données incluses dans le datagramme.

Encapsulating Security Payload (ESP)

Le protocole ESP (Encapsulating Security Payload) a lui été conçu pour assurer la confidentialité des données. Mais il peut aussi apporter des services d'intégrité en mode non connecté, d'authentification de l'origine des données, et un service anti-rejeu optionnel. Le principe d'ESP est de générer, à partir d'un datagramme IP classique, un nouveau datagramme dans lequel les données et éventuellement l'entête original sont chiffrés.

Seul le protocole ESP en mode tunnel (cf section mode d'utilisation) est supporté par l'IPS-Firewall NETASQ.

© Copyright NETASQ 2006

Modes d'utilisation

Pour chacun des mécanismes de sécurité d'IPSEC, il existe deux modes : le mode transport et le mode tunnel.

En mode transport, seules les données en provenance du protocole de niveau supérieur et transportées par le datagramme IP sont protégées. Ce mode n'est utilisable que sur des équipements terminaux.

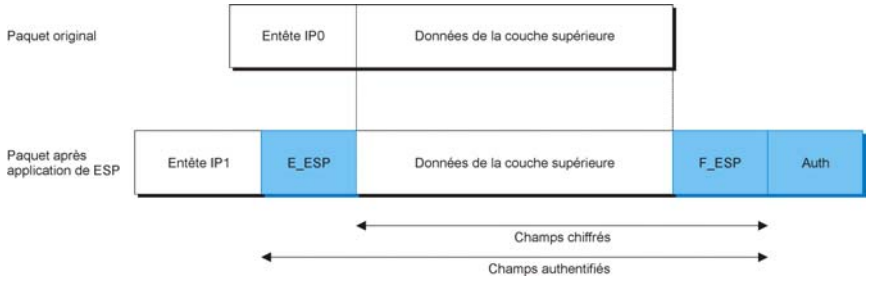
En mode tunnel, l'en-tête IP est également protégé (authentification, intégrité et/ou confidentialité) et remplacé par un nouvel en-tête. Ce nouvel en-tête sert à transporter le paquet jusqu'à la fin du tunnel, où l'en-tête original est rétabli. Le mode tunnel est utilisable soit sur des équipements terminaux soit au niveau de passerelles de sécurité. Ce mode permet d'assurer une protection plus importante contre l'analyse du trafic.

Les exemples suivants montrent dans le cas de l'ESP (Encapsulating Security Payload) les différences entre les deux modes d'utilisation.

Rappel : seul le protocole ESP en mode tunnel est supporté par l'IPS-Firewall NETASQ.

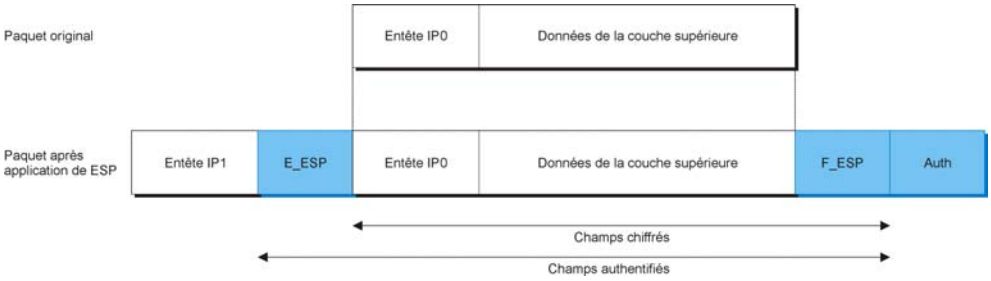
ESP mode transport

Protection de bout en bout (adresses sources et destination non modifiées)



ESP mode tunnel

A utiliser pour protéger le trafic entre deux éléments de coupure



Le choix de NETASQ

Comme indiqué ci-dessus, les fonctionnalités d'un IPS-Firewall NETASQ implémentent uniquement le protocole ESP d'IPSEC pour fournir des services d'authentification et de chiffrement des datagrammes échangés avec un correspondant VPN (qui peut être éventuellement un autre IPS-Firewall), possédant des fonctionnalités homologues.

De plus un IPS-Firewall NETASQ met en œuvre le protocole ESP uniquement en mode tunnel. Cela implique que les fonctions de chiffrement ne peuvent pas être mises en œuvre de bout en bout, mais uniquement sur une portion du réseau qui supporte le flux, physiquement délimitée par les correspondants VPN, typiquement le réseau dit « Untrusted » (non sûr). Sur cette portion les datagrammes IP à protéger sont intégralement chiffrés, signés et encapsulés dans des datagrammes ESP dont les adresses IP source et destination sont celles des correspondants VPN. Ainsi les adresses IP des machines réelles d'extrémité du flux sont inaccessibles à des attaquants à l'écoute sur le réseau non sûr. Les correspondants VPN sont appelés extrémités du tunnel, par opposition aux machines réelles d'extrémité du flux, situées « derrière » les correspondants VPN du point de vue réseau non sûr et qu'on appelle les extrémités de trafic.

Le fait d'avoir privilégié le protocole ESP en mode tunnel est basé sur **deux constats**.

Schématiquement on peut associer le **mode transport** à une utilisation dite « host to host » un trafic de bout en bout, d'une machine unique vers une machine unique. Tandis que le mode tunnel est plutôt utilisé dans un cadre dit « network to network » c'est à dire un groupe de machines vers un groupe de machines. Cette configuration correspond plus au type d'architecture rencontrée dans le cadre de l'utilisation d'un IPS-Firewall, étant donné qu'un IPS-Firewall est généralement utilisé pour protéger un réseau. Ainsi NETASQ privilégiera le mode tunnel.

De plus on peut imaginer dans une certaine mesure que le mode transport soit en réalité un cas d'utilisation du mode tunnel (les extrémités de tunnel et de trafic sont confondues). Mais ce cas n'est pas supporté sur un IPS-Firewall NETASQ.

Etant donné que NETASQ a choisi de n'implémenter que le mode tunnel sur son IPS-Firewall, les développements sur **l'AH (Authentication Header)** ont été interrompu. En effet dans le cadre du mode tunnel seules trois informations « sensibles » nécessiterait le besoin d'une authentification : les adresses source et destination et l'index de sécurité (SPI : Security Policy Indentifier) de la SA (Security Association) associée. Hors ces informations sont indispensables au fonctionnement de la politique VPN. La modification d'un de ces paramètres entraîne irrémédiablement le rejet du paquet par le correspondant. L'utilisation d'AH dans le cadre du mode tunnel devient alors inutile par rapport ESP.

Différentes phases

Dans le cadre d'ESP (AH aussi d'ailleurs mais seul ESP nous intéresse dans le cadre d'un IPS-Firewall NETASQ), chaque datagramme échangé entre deux correspondants VPN donnés est rattaché à une connexion simplex ou unidirectionnelle (en fonction du point de vue elle est donc soit entrante soit sortante) mettant en œuvre des services de sécurité, appelée Association de Sécurité IPSEC (SA : Security Association). Une SA IPSEC spécifie les algorithmes de chiffrement et d'authentification à appliquer sur les datagrammes qu'elle couvre, ainsi que les clés secrètes associées.

Le déploiement et l'utilisation massive d'IPsec exige un protocole de gestion des SA standard sur Internet, extensible et automatisé. Par défaut, le protocole de gestion automatisée des clefs choisi pour IPsec est IKE. IKE est organisé autour de 2 phases de négociation.

La phase 1 du protocole IKE vise à établir un canal de communication chiffré et authentifié entre les deux correspondants VPN. Ce « canal » est appelé SA ISAKMP (différent de la SA IPSEC). Deux modes de négociations sont possibles : le mode principal et le mode agressif.

La phase 2 du protocole IKE négocie de manière sécurisée (au moyen du canal de communication SA ISAKMP négocié dans la première phase) les paramètres de la futur SA IPSEC.

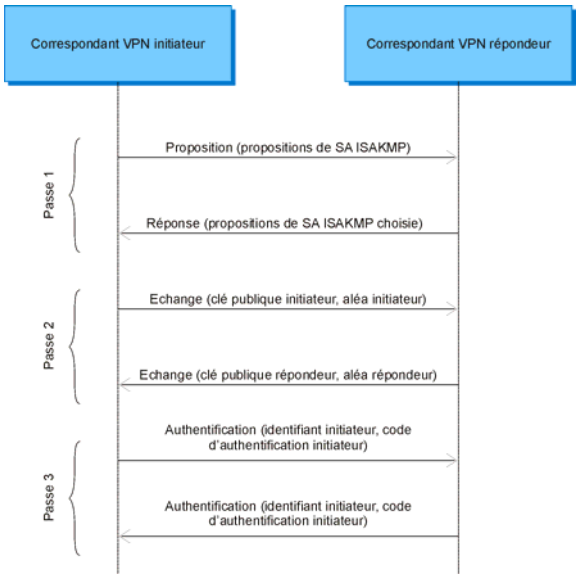
Phase 1 du protocole IKE

La phase 1 du protocole IKE concourt à trois objectifs :

► la négociation des paramètres de la SA ISAKMP,
► l'élaboration des clés secrètes d'authentification, de chiffrement et de dérivation de la SA ISAKMP,
► l'authentification mutuelle des correspondants VPN.

Dans le cadre d'un IPS-Firewall NETASQ, les fonctions d'établissement de SA n'acceptent des négociations de SA ISAKMP qu'avec des correspondants VPN pour lesquels un tunnel est défini dans le slot de chiffrement courant et ce sur l'interface réseaux spécifiée pour ce tunnel.

Le diagramme suivant représente les étapes de la négociation en mode principal utilisant une clé pré partagée (pre-shared key).


Correspondant VPN initiateur
Correspondant VPN répondeur
Passe 1
Proposition (propositions de SA ISAKMP)
Réponse (propositions de SA ISAKMP choisie)
Passe 2
Echange (clé publique initiateur, aléa initiateur)
Echange (clé publique répondeur, aléa répondeur)
Passe 3
Authentification (identifiant initiateur, code d'authentification initiateur)
Authentification (identifiant initiateur, code d'authentification initiateur)

La passe 1 correspond à la négociation de la SA ISAKMP. Chaque règle de chiffrement possède une liste de propositions de SA ISAKMP qui sont des quintuplés de la forme (durée de vie de la SA, algorithme d'authentification, taille de clé d'authentification, algorithme de chiffrement, taille de clé de chiffrement).

La passe 2 permet d'élaborer un secret partagé, dont on dérive la clé secrète d'authentification et la clé secrète de chiffrement de la SA ISAKMP, utilisables par les services négociés en passe 1. Une clé secrète de dérivation utilisée en phase 2 IKE est également générée.

La passe 3, protégée par les services d'authentification et de chiffrement, permet l'authentification mutuelle des correspondants VPN. Le code d'authentification de chaque correspondant VPN est généré à partir de la clé pré-partagée, du secret partagé, des aléas et de l'identifiant du correspondant VPN.

D'autres modes de négociation et méthodes d'authentification sont supportés par l'IPS-Firewall : mode agressif ou mode principal et authentification par clés pré-partagées ou par certificat X509.

Mode agressif ou mode principal

Le mode agressif s'effectue en trois étapes :

► la première étape combine la proposition, l'échange de clé initiateur et l'envoi de l'identification de l'initiateur,

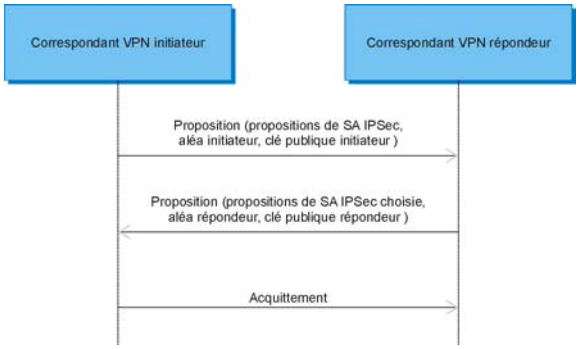
► la deuxième étape combine la réponse, l'échange de clé répondeur et l'authentification du répondeur,
► la troisième étape consiste pour l'initiateur à envoyer son code d'authentification.

Clés pré-partagées ou certificats X509

En utilisant les certificats X509 en mode principal, l'identifiant de chaque correspondant VPN est communiqué lors de la passe 2. Que ce soit en mode principal ou en mode agressif, chaque correspondant VPN chiffre son identifiant avec la clé publique de son vis-à-vis. Le code d'authentification de chaque correspondant VPN est généré à partir du secret pré-partagé, des aléas et de l'identifiant du correspondant. Mais les aléas sont également chiffrés, quand ils sont envoyés au cours de l'étape d'échange de clé, avec la clé publique du vis-à-vis, ce qui permet l'authentification de celui-ci.

Phase 2 du protocole IKE

L'établissement d'une SA IPSEC entre deux correspondants VPN nécessite une phase de négociation des paramètres et d'établissement des clés afin d'assurer que les deux extrémités du tunnel appliquent la règle de chiffrement associée à la SA IPSEC de manière cohérente. La négociation des SA IPSEC est basée sur la phase 2 (Quick mode) du protocole IKE. De manière simplifiée, les étapes de cette négociation peuvent être représentées par le diagramme de séquence suivant.


Correspondant VPN initiateur
Correspondant VPN répondeur
Proposition (propositions de SA IPSec, aléa initiateur, clé publique initiateur)
Proposition (propositions de SA IPSec choisie, aléa répondeur, clé publique répondeur)
Acquittement

Tous les échanges sont chiffrés et authentifiés par les services fournis par la SA ISAKMP, négociée et établie entre les correspondants VPN préalablement à l'établissement des SA IPSec associées aux règles de chiffrement.

Chaque règle de chiffrement possède une liste de propositions de SA IPSec qui sont des quintuplés de la même forme que pour la négociation des SA ISAKMP.

Lors de la deuxième étape de la phase 2 du protocole IKE, le répondeur doit choisir et recopier dans sa réponse une des propositions qui lui a été soumise, sinon l'initiateur refuse la négociation. En situation de répondeur, l'IPS-Firewall NETASQ applique les règles suivantes pour sélectionner la réponse :

► la réponse choisie est la première qui correspond à la stratégie de négociation spécifiée au niveau du tunnel,

► la stratégie de négociation peut être « exacte » ou « stricte ». En cas de stratégie exacte, une proposition de l'initiateur correspond à une proposition locale si elle lui est exactement égale. En cas de stratégie stricte, une proposition de l'initiateur correspond à une proposition locale si elle lui est égale ou supérieure,

Une proposition de l'initiateur est égale ou supérieure à une proposition locale si les conditions du tableau ci-dessous sont réalisées :

Attrib. de la proposition initiateur	Relation	Attrib. de la proposition locale
Durée de vie	≤	Durée de vie

Algorithme d'authentification	=	Algorithme d'authentification
Taille de clé d'authentification	≥	Taille de clé d'authentification
Algorithme de chiffrement	=	Algorithme de chiffrement
Taille de clé de chiffrement	≥	Taille de clé de chiffrement
Perfect Forward Secrecy	≥	Perfect Forward Secrecy

En cas de stratégie stricte, il peut donc arriver que les attributs d'une SA soient différents de ceux des propositions locales associées à la règle de chiffrement utilisant la SA.

Suite à la réussite de la négociation, les clés d'authentification et de chiffrement sont élaborées à partir des clés publiques (secret partagé Diffie-Hellman), des aléas et des autres paramètres échangés lors de la phase 2, ainsi que d'une clé secrète de dérivation élaborée lors de la phase 1.

Certificats X509

La solution IPS-Firewall NETASQ supporte et utilise deux méthodes d'authentification : les clés pré-partagées et les certificats X509. Les deux méthodes possèdent le même niveau de sécurité mais leur gestion est différente. Cette distinction est abordée dans la configuration des politiques VPN (cf. Création d'un tunnel VPN).

La sécurisation des flux d'information à l'aide de certificats est un élément parmi d'autres de la politique de sécurité de l'entreprise. Cette politique doit être réfléchie et définie dans un manuel officiel, reflet de la mise en sécurité globale de l'entreprise. L'ensemble des configurations d'IPSec (certificat ou clé pré-partagée, durée de vie de SA, choix des algorithmes, ...) représente un niveau de sécurité : ce dernier est toujours défini à bon escient, proportionnel à la valeur de ce qu'il protège.

Cette section se focalise sur l'authentification des correspondants VPN par certificat.

Elle n'a pas pour vocation d'offrir une explication complète ou exhaustive des infrastructures à clé publique, mais d'expliquer la configuration ISAKMP par certificats dans un IPS-Firewall NETASQ.

Génération des certificats

Un IPS-Firewall NETASQ contient une infrastructure à clé publique interne qui vous permet de créer les certificats des utilisateurs de votre système d'information mais il peut aussi intégrer les fichiers générés par une PKI externe privée (ex: openSSL, CMS d'iPlanet, Baltimore,...) ou officielle (ex: Thawte, Verisign, ...).

La procédure à suivre pour générer des certificats externes se déroule selon des formalités décrites dans les manuels des éditeurs de la solution PKI privée ou sur les sites web des CA officielles.

Les étapes pour la génération d'un certificat local et la configuration d'un IPS-Firewall sont :

- ► génération d'une paire de clés (appelée aussi biclé),
- ► importation de la clé privée dans l'IPS-Firewall,
- ► envoi d'une requête de demande de certificat (accompagné de la clé publique) à la CA,
- ► récupération du certificat auprès de la CA après validation par celle-ci,
- ► importation du certificat dans l'IPS-Firewall,
- ► récupération et importation du certificat de la CA,
- ► récupération et importation des certificats des correspondants.

Donc, pour configurer l'IPS-Firewall, il faut importer différents fichiers (trois catégories de certificats, les clés privées et liste de révocation). Chaque fichier contient un des éléments cités ci-dessous.

Clé privée

De la paire de clés générée par la PKI, l'IPS-Firewall doit posséder l'exemplaire privé et public. L'IPS-Firewall ne génère pas lui même la paire de clés, c'est la PKI qui le fait. La clé publique étant située dans le certificat, il convient donc d'importer la clé privée dans le document.

Cette clé privée permettra de signer les informations envoyées.

Cette clé est générée en même temps que la clé publique par l'administrateur en vue de la génération du certificat pour l'IPS-Firewall local.

Certificat de firewall local

Ce certificat est généré pour l'IPS-Firewall local. La clé publique qu'il contient permettra l'authentification avec les IPS-Firewalls correspondants.

Ces certificats sont générés par l'administrateur pour l'IPS-Firewall local.

Certificats des correspondants

Ces certificats sont générés par les IPS-Firewalls distants. La clé publique qu'il contient permettra l'authentification des IPS-Firewalls correspondants.

Ces certificats sont fournis par l'administrateur des IPS-Firewalls distants.

Certificats des CA

Ils sont générés par les CA. La clé publique qu'ils contiennent permettra de vérifier la validité des certificats des firewalls distants (certificats des correspondants) et ceux du firewall local.

Ces certificats sont le plus souvent récupérables, soit dans l'application PKI privée, soit sur le site de la CA officielle.

Liste de révocation

Chaque certificat peut être annulé (révoqué) lorsque des responsables (administrateurs, chefs de services ou d'entreprise, ... selon les cas) décident que tel ou tel certificat n'assure plus ou met en péril la sécurité des transactions. En effet, des certificats peuvent créer des failles de sécurité dans divers cas de figure tels que la perte ou vol de la clé privée, le départ de l'administrateur de l'IPS-Firewall ou peuvent être associé à des personnes qui ne sont plus autorisées à accéder à ce système. Les PKI permettent de révoquer des certificats, générer, exporter et publier des listes contenant les certificats révoqués. Cette liste doit être mise à jour automatiquement et périodiquement consultée par l'IPS-Firewall, dans le cas contraire, certaines personnes ou ressources pourraient conserver des accès auxquels elles n'ont plus droit.

Formats reconnus par un IPS-Firewall NETASQ

- PEM (Privacy Enhanced Mail) . Il permet l'encodage des certificats X509 en base 64,
- DER, format binaire,
- PKCS#12.

Pour exemple, un certificat de type PEM se présente de la manière suivante :

-----BEGIN CERTIFICATE-----
MIIDdzCCAuCgAwIBAgIBBzANBgkqhkiG9w0BAQQFADCBpDELMAkGA1UEBhMCQ0gxCzAJBgN
VBAgTAkdFMQ8wDQYDVQQHEwZHZW5ldmExHTAbBgNVBAoTFFVuaXZlcnNpdHkgb2YgR2VuZ
XZhMSQwIgYDVQQLExtVTklHRSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkxETAPBgNVBAMTCFV
uaUdlIENBMR8wHQYJKoZIhvcNAQkBFhB1bmlnZWNhQHVuaWdlLmNoMB4XDTk5MTAwNDE2Mj
I1N1oXDTAwMTAwMzE2MjI1N1owgbExCzAJBgNVBAYTAkNIMQswCQYDVQQIEwJHRTEPMA0G
A1UEBxMGR2VuZXZhMR0wGwYDVQQKExRVbml2ZXJzaXR5IG9mIEdlbmV2YTEeMBwGA1UEC
xMVRGl2aXNpb24gSW5mb3JtYXRpcXVlMRowGAYDVQQDExFBbGFpbiBIdWdlbnRvYmxlcjEpMC
cGCSqGSIb3DQEJARYaQWxhaW4uSHVnZW50b2JsZXJAdW5pZ2UuY2gwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBALIL5oX/FR9ioQHM0aXxfDELkhPKkw8jc6I7BtSYJk4sfqvQYqvOMt1u
ugQGkyIuGhP2djLj6Ju4+KyKKQVvDJIu/R1zFX1kkqOPt/A2pCLkisuH7nDsMbWbep0hDTVNELoKV
oVIAazwWMFlno2JuHJgUcs5hWskg/azqI4d9zy5AgMBAAGjgakwgaYwJQYDVR0RBB4wHIEaQWx
haW4uSHVnZW50b2JsZXJAdW5pZ2UuY2gwDAYDVR0T200BAUwAwIBADBcBglghkgBhvhCAQ0
ETxZNVU5JR0VDQSBjbGllbnQgY2VydGlmaWNhdGUsIHNlZSBodHRwOi8vdW5pZ2VjYS51bmlnZ

S5jaCBmb3IgbW9yZSBpbmZvcm1hdGlvbnMwEQYJYIZIAYb4QgEBBAQDAgSwMA0GCSqGSIb3D
QEBBAUAA4GBACQ9Eo67A3UUa6QBBNJYbGhC7zSjXiWySvj6k4az2UqTOCT9mCNnmPR5I3Kx
r1GpWToH68LvA30inskP9rkZAksPyaZzjT7aL//phV3ViJfreGbVs5tiT/cmigwFLeUWFRvNyT9VUPUo
v9hGVbCc9x+v05uY7t3UMeZejj8zHHM+
-----END CERTIFICATE-----

Les balises "-----BEGIN CERTIFICATE-----" et "-----END CERTIFICATE-----" encadrent le bloc de "n" lignes de chacune 64 caractères de type [A-Za-z0-9/+].

C'est un format qui transite souvent par e-mail car celui-ci résiste très bien aux déformations des logiciels de messagerie.

Le fichier PEM est un fichier texte contenant ce type d'information.

De même le fichier CRL contient des chaînes de caractères codées en base 64 encadrées par des balises du type : "-----BEGIN X509 CRL-----" et "-----END X509 CRL-----".

Le fichier de clé privée, quant à lui, contient des chaînes de caractères codées en base 64 encadrées par des balises du type : "-----BEGIN RSA PRIVATE KEY-----" et "-----END RSA PRIVATE KEY-----".

Les incompatibilités connues entre la translation d'adresses (NAT : Network Address Translation) et les tunnels VPN (VPN : Virtual Private Network) IPsec entraînent des problèmes souvent bloquants lors de l'établissement de tunnel VPN IPsec au travers d'équipement effectuant des opérations de NAT.

Le NAT-T permet de supporter un trafic VPN transitant au travers de routeur réalisant de la translation d'adresse. Le nombre d'équipements réalisant une translation n'est pas une limite de la fonctionnalité chez NETASQ. NETASQ est compatible avec tous les DRAFTs et RFC rédigés sur les fonctionnalités.

Incompatibilités connues entre la translation d'adresses (NAT) et l'IPsec

Ces incompatibilités entre le NAT et l'IPsec peuvent être divisées en trois catégories :

► Les problèmes intrinsèques au NAT. Ces incompatibilités dérivent directement des fonctionnalités de translation d'adresses. Ces incompatibilités seront donc présentes dans tous les équipements fournissant du NAT.

► Les faiblesses d'implémentation du NAT. Ces incompatibilités ne sont pas intrinsèques au NAT, mais sont présentes dans de nombreuses implémentations.

► Les solutions propriétaires. Ces incompatibilités sont présentes dans les équipements NAT qui tentent de fournir des fonctionnalités permettant le passage de l'IPsec au travers du NAT. Ironiquement, ces fonctionnalités créent encore plus d'incompatibilités, étant donné qu'elles ont été développées sur des technologies propriétaires.

Problèmes intrinsèques au NAT

Les incompatibilités entre l'AH IPsec et le NAT

Etant donné que l'entête AH intègre les adresses IP source et destination dans la vérification de l'intégrité des messages, les équipements NAT modifiant les champs d'adresses invalident la vérification de l'intégrité des messages. L'ESP IPsec n'intègre pas les adresses IP source et destination dans sa vérification optionnelle de l'intégrité chiffrée du message, ce problème ne se pose donc pas pour l'ESP.

Incompatibilité entre les sommes de contrôle et le NAT

Les sommes de contrôles TCP et UDP sont dépendantes des adresses IP source et destination par l'intégration de l'entête dans leur calcul. Ainsi, lorsque les sommes de contrôle sont calculées et vérifiées à la réception, ils sont invalidés lors d'un passage au travers d'un équipement NAT.

Ainsi seul, l'IPsec Encapsulating Security Payload (ESP) sera capable de passer sans difficulté au travers d'un équipement NAT si les protocoles TPC/UDP ne sont pas impliqués, ou si les sommes de contrôles ne sont pas calculées.

Incompatibilité entre les identifiants d'adresses IKE et le NAT

Lorsque les adresses IP sont utilisées comme identifiants dans la phase 1 du protocole IKE (Internet Key Exchange), la modification des adresses IP source et destination par le NAT résultera d'une erreur entre les identifiants et les adresses dans les entêtes IP.

Pour éviter d'utiliser les adresses IP comme identifiants de phase 1, les UserID et les FQDN peuvent être utilisés. Lorsque l'authentification d'un utilisateur est demandée, on utilisera le type d'ID ID_USER_FQDN. Lorsque l'authentification d'une machine est demandée, on utilisera le type

© Copyright NETASQ 2006

d'ID ID_FQDN. Dans les deux cas, il est nécessaire de vérifier que l'identifiant proposé est authentifié par un certificat si des certificats sont échangés dans la phase 1.

Les incompatibilités entre le port source fixé de l'IKE et le NAT

Lorsque de multiples hôtes derrière un équipement de NAT initient des SA IKE vers le même correspondant, un mécanisme est nécessaire pour permettre à l'équipement NAT de démultiplexer les paquets IKE entrants provenant du correspondant. Cela est typiquement réalisé par une translation du port source UDP IKE des paquets sortants de l'initiateur. Ainsi les correspondants doivent être capable d'accepter un trafic IKE provenant d'un port différent du port 500 et doivent répondre sur ce port. De plus il est important de faire attention à ce mécanisme pour éviter les comportements imprévisibles durant la renégociation des clés. Si le port source flottant n'est pas utilisé comme port destination pour la renégociation des clés, le NAT sera incapable d'envoyer les paquets renégociés vers la destination correcte.

Les incompatibilités entre la sélection des SPI IPsec et le NAT

Comme le trafic ESP IPsec est chiffré, il est donc opaque au NAT, le NAT est obligé d'utiliser des éléments des entêtes IP et IPsec pour démultiplexer les trafics IPsec entrants. La combinaison de l'adresse IP de destination, le protocole de sécurité (AH/ESP) et le SPI IPSec est typiquement utilisé dans ce but.

Cependant, comme les SPI entrantes et sortantes sont choisis indépendamment, il n'y a aucun moyen pour le NAT de déterminer quel SPI entrant correspond à quel hôte de destination simplement en inspectant le trafic sortant. Ainsi lorsque deux hôtes derrière le NAT tentent de créer des SA IPsec avec la même destination simultanément, il est possible que le NAT délivre les paquets IPsec entrants vers la mauvaise destination.

Les incompatibilités entre les adresses IP embarquées et le NAT

Comme l'intégrité du payload est protégée, toutes les adresses IP incluses dans les paquets IPsec ne peuvent être translatées par un équipement de NAT. Ceci rend ineffective les passerelles de couche applicative (ALG : Application Layer Gateway) implémentées avec du NAT. Les protocoles qui utilisent des adresses IP embarquées incluent FTP, IRC, SNMP, LDAP, H323, SIP, SCTP (de façon optionnelle) et de nombreux jeux. Pour répondre à ce problème, il est nécessaire d'installer l'ALG sur un hôte ou une passerelle de sécurité qui puisse traiter le trafic applicatif avant l'encapsulation IPsec et après la désencapsulation IPsec.

Directionnalité implicite du NAT

Les équipements de NAT requièrent souvent un paquet initial sortant pour les traverser dans le but de créer une table de mapping entrant. La directionnalité du protocole interdit l'établissement non sollicité de SA IPsec vers des hôtes situés derrière un équipement de NAT.

Faiblesses d'implémentation du NAT

L'incapacité à pouvoir traiter les trafics non UDP/TCP

Certaines implémentations du NAT supprime les trafics non UDP/TCP ou réalisent uniquement une translation d'adresse lorsqu'un seul hôte se situe derrière l'équipement de NAT. De telles implémentations sont donc incapables d'accepter les trafics des protocoles ESP ou AH.

Les timeouts des « sessions » NAT

Les équipements de NAT ne sont pas homogènes dans leur gestion des durées de maintien des « sessions » UDP en l'absence de trafic. Ainsi, même lorsque les paquets IKE sont correctement translatés, les sessions de translation peuvent être prématurément supprimées.

Incapacité à traiter les fragments sortants

La plupart des équipements NAT peuvent fragmenter proprement les paquets IP sortants dans le cas où la taille des paquets IP dépasse le MTU de l'interface sortante. Cependant, une translation correcte des paquets sortants qui sont déjà fragmentés est difficile et la plupart des équipements NAT ne traitent pas correctement ces trafics. Lorsque deux hôtes génèrent des paquets fragmentés vers la même destination, les identifiants de fragments peuvent se recouvrir. Etant donné que l'hôte

de destination se base sur les identifiants de fragmentation et le décalage des fragments pour le réassemblage, cela peut provoquer une corruption des données.

Incapacité à traiter les fragments entrants

De la même façon que pour les fragments sortants, le morcelage des adresses IP et des entêtes nécessaires à la translation peut nécessiter un réassemblage complet des fragments compliqué par une arrivée désordonnée des fragments.

Les solutions propriétaires

Vérification de l'entête des paquets ISAKMP

Certaines implémentations tentent d'utiliser les cookies IKE pour démultiplexer les trafics IKE entrants. Comme avec le démultiplexage basé sur le port source, le démultiplexage basé sur les cookies IKE subit les problèmes de la renégociation des clés, étant donné qu'une renégociation des clés en phase1 n'utilisera typiquement pas les mêmes cookies que le trafic précédent.

Traitement spécifique sur le port 500

Etant donné que certaines implémentations d'IKE sont incapables d'utiliser des ports sources différents du port UDP 500, certains équipements de NAT ne translatent pas les paquets avec un port source UDP 500. Ceci signifie que ces équipements de NAT sont limités à un client IPsec par passerelle de destination, à moins qu'ils n'inspectent les détails de l'entête ISAKMP pour examiner les cookies qui créent le problème noté plus haut.

Vérification du payload ISAKMP

Les implémentations de NAT qui tentent d'analyser les payloads ISAKMP ne peuvent pas traiter tous les envois de combinaisons de payload ou de Vendor_ID possibles de la négociation des options IKE.

Fonctionnement du NAT-Traversal

La détection du support du NAT-Traversal et la détection du NAT sur le chemin entre deux correspondants IKE se situe dans la phase 1 IKE.

Le NAT-Traversal utilise plusieurs méthodes pour permettre le passage de l'IPSEC au travers du NAT. Le changement de port (ou port floating) pour contourner les solutions propriétaires, l'encapsulation de l'ESP dans l'UDP pour permettre la différenciation des correspondants IPSEC et de leur trafic et enfin l'envoi régulier de KEEPALIVE permettant la conservation de la session NAT.

Détection du support du NAT-Traversal

La capacité d'un hôte à supporter le NAT-Traversal est déterminée par un échange de Payloads Vendor_ID. Les payloads Vendor_ID du NAT-T doivent être envoyés lors du premier échange de paquets de la phase 1 (et ils doivent être reçus par les deux correspondants) pour continuer à utiliser le NAT-T. Un payload pour chaque version du NAT-T supportée sera envoyé. Le contenu de ce payload est un hash MD5 de « RFC 3947 », la valeur de ce payload est 4a131c81070358455c5728f20e95452f.

Détection de la présence du NAT

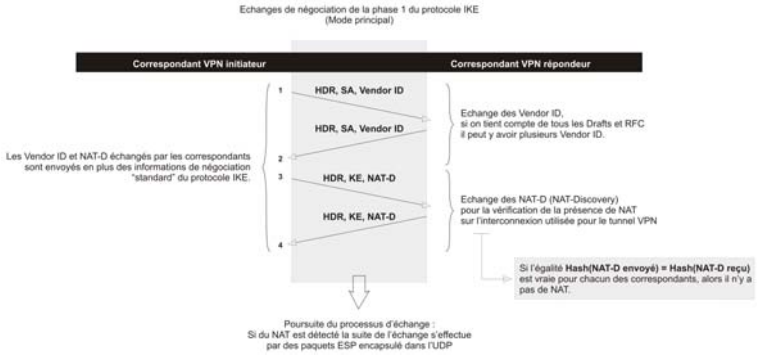
Le NAT-T ne détecte pas seulement la présence du NAT entre deux correspondants IKE, mais détecte aussi où se trouve le NAT. Localiser l'équipement de NAT est important, étant donné que des « KEEPALIVE » doivent être initiés par le correspondant situé derrière le NAT.

Pour détecter du NAT entre les deux correspondants, il est nécessaire de détecter si l'adresse IP ou le port changent au cours du trajet (cela implique que les destinataires doivent être capables de traiter des paquets IKE dont le port source est différent du port 500 habituel).

Les correspondants envoient à leur vis à vis un hash des ports et adresses IP. Si lorsque chacun des correspondants recalculent le hash (à partir des ports et adresses IP qu'ils reçoivent), celui-ci correspond au hash envoyé par leur vis à vis alors il n'y a pas de NAT entre eux. Si les hashes ne correspondent pas, alors quelqu'un a translaté l'adresse ou le port. Ce qui signifie que du NAT-Traversal doit être fait pour que les paquets IPsec puisse traverser.

Les hashs sont envoyés comme une série de payloads NAT-D (NAT Discovery) inclus dans le troisième et quatrième paquet du mode principal et dans le second et le troisième paquet du mode agressif.

L'exemple suivant montre un échange de payloads NAT-D en mode principal :


Echanges de négociation de la phase 1 du protocole IKE
(Mode principal)
Correspondant VPN initiateur
Correspondant VPN répondeur
1
HDR, SA, Vendor ID
HDR, SA, Vendor ID
Echange des Vendor ID,
si on tient compte de tous les Drafts et RFC
il peut y avoir plusieurs Vendor ID.
Les Vendor ID et NAT-D échangés par les correspondants
sont envoyés en plus des informations de négociation
"standard" du protocole IKE.
2
3
HDR, KE, NAT-D
HDR, KE, NAT-D
Echange des NAT-D (NAT-Discovery)
pour la vérification de la présence de NAT
sur l'interconnexion utilisée pour le tunnel VPN
4
Si l'égalité Hash(NAT-D envoyé) = Hash(NAT-D reçu)
est vraie pour chacun des correspondants, alors il n'y a
pas de NAT.
Poursuite du processus d'échange :
Si du NAT est détecté la suite de l'échange s'effectue
par des paquets ESP encapsulé dans l'UDP

Le format d'un payload NAT-D est le suivant :

```
                    1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2
+---------------+---------------+---------------+---------------+
| Next Payload  | RESERVED      | Payload Length                |
+---------------+---------------+---------------+---------------+
~                HASH of the address and port                   ~
+---------------+---------------+---------------+---------------+
```

NAT-D packet format

Le type du payload pour le payload du NAT-D (NAT Discovery) est 20.

Le hash est calculé de la manière suivante : HASH = HASH(CKY-I | CKY-R | IP | Port).

Ceci utilise l'algorithme de HASH précédemment négocié (les hashes sont envoyés dans le troisième et le quatrième paquet, les SA négociant les algorithmes de chiffrement et d'authentification sont envoyés dans le premier et le deuxième paquet). Le premier payload NAT-D contient l'adresse IP et le port de l'extrémité de tunnel distante (c'est-à-dire, l'adresse de destination des paquets UDP). Les payload NAT-D suivant contiennent les adresses IP et ports des différentes extrémités de tunnel locales possibles (c'est-à-dire toutes les sources possibles des paquets UDP).

S'il n'y a pas de NAT entre les correspondants, le premier payload NAT-D reçu par un hôte doit correspondre au payload NAT-D local (c'est-à-dire le payload NAT-D local qu'envoie cet hôte à son correspondant), et un des autres payloads NAT-D doit correspondre à l'adresse IP et port du correspondant. Si la première vérification échoue (c'est-à-dire, que le premier des payload NAT-D ne correspond à aucune adresse IP et port local), cela signifie qu'il y a de la translation dynamique entre les correspondants et que cette extrémité de tunnel doit commencer à envoyer des KEEPALIVE (car cette extrémité se trouve derrière un équipement de NAT).

Le CKY-I et CKY-R sont les cookies de l'initiateur et du répondeur. Ils ont été ajoutés au hash pour protéger les adresses IP et port contre les attaques.

Changement vers un nouveau port

Les interactions IPsec et du NAT intelligent peuvent poser des problèmes. Certains équipements de NAT ne changeront pas le port source IKE (500) même s'il y a plusieurs clients derrière le NAT. Ils peuvent aussi utiliser les cookies IKE pour démultiplexer le trafic au lieu d'utiliser le port source. Les deux cas posent le problème de la transparence du NAT, qui engendre des problèmes pour la découverte par IKE des capacités de NAT des équipements traversés par le trafic. La meilleure approche consiste à simplement déplacer le trafic IKE vers un autre port que le 500 le plus vite possible pour éviter ces cas spéciaux de NAT intelligent.

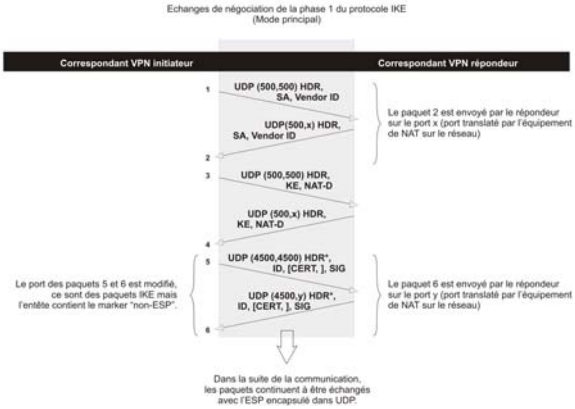
© Copyright NETASQ 2006

Prenant en compte le cas le plus courant où l'initiateur se trouve derrière un équipement de NAT. L'initiateur doit rapidement changer vers le port UDP 4500 une fois que le NAT a été détecté pour minimiser la fenêtre des problèmes d'interactions IPsec et NAT intelligent.

Lorsque le répondeur reçoit ce paquet, le déchiffrement et les traitements habituels sont effectués sur les différents payloads. S'ils sont effectués avec succès, le répondeur doit mettre à jour sa table locale pour que tous les paquets suivants (les notifications d'informations incluses) à destination du correspondant utiliseront le nouveau port et éventuellement la nouvelle adresse IP obtenues du paquet reçu. Le port sera généralement différent, ainsi le NAT effectuera un map UDP(500, 500) vers UDP(x, 500) et UDP(4500, 4500) vers UDP(y, 4500). L'adresse IP sera rarement différente de l'adresse IP précédente. Le répondeur renvoie tous les paquets IKE suivants vers son correspondant en utilisant UDP(4500, y).

De la même façon, si le répondeur doit rénégocier la SA de phase 1, alors la négociation démarre en utilisant UDP(4500, y). Si une négociation démarre sur le port 4500, alors il n'est pas nécessaire de changer quoique ce soit dans le reste de l'échange.

Voici un exemple d'échange de phase 1 utilisant du NAT-Traversal en mode principal avec un changement de port :


Echanges de négociation de la phase 1 du protocole IKE
(Mode principal)
Correspondant VPN initiateur
Correspondant VPN répondeur
1
UDP (500,500) HDR, SA, Vendor ID
UDP(500,x) HDR, SA, Vendor ID
Le paquet 2 est envoyé par le répondeur sur le port x (port translaté par l'équipement de NAT sur le réseau)
2
3
UDP (500,500) HDR, KE, NAT-D
UDP (500,x) HDR, KE, NAT-D
4
5
UDP (4500,4500) HDR*, ID, [CERT,], SIG
UDP (4500,y) HDR*, ID, [CERT,], SIG
Le port des paquets 5 et 6 est modifié, ce sont des paquets IKE mais l'entête contient le marker "non-ESP".
Le paquet 6 est envoyé par le répondeur sur le port y (port translaté par l'équipement de NAT sur le réseau)
6
Dans la suite de la communication, les paquets continuent à être échangés avec l'ESP encapsulé dans UDP.

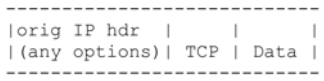
Encapsulation du trafic ESP dans l'UDP

Du fait des « incompatibilités entre la sélection des SPI IPsec et le NAT » (explications au début du document), il est indispensable de mettre en place un mécanisme permettant la distinction des différents trafics VPN. L'encapsulation du trafic ESP dans un protocole « plus classique » comme l'UDP permet de créer une certaine concordance entre les différents trafics VPN représentés par leur SPI et un élément de l'entête UDP que les équipements effectuant du NAT sauront traiter, en l'occurrence les ports.

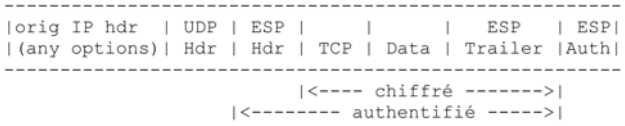
Ainsi dès que la négociation VPN est terminée, l'ensemble du trafic ESP est encapsulé dans l'UDP comme le montrent les différents schémas suivants :

Encapsulation du trafic ESP en mode transport

Paquet avant encapsulation dans l'ESP et l'UDP

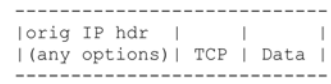


Paquet après encapsulation dans l'ESP et l'UDP



Encapsulation du trafic ESP en mode tunnel

Paquet avant encapsulation dans l'ESP et l'UDP

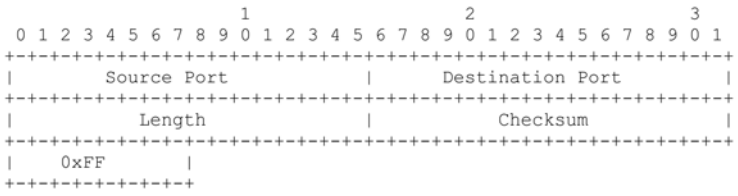


Paquet après encapsulation dans l'ESP et l'UDP

Préservation de la pseudo session NAT

La stabilité du tunnel VPN IPsec est garantie par la préservation de la session NAT, obtenue grâce à l'envoi régulier de KEEPALIVE entre les deux correspondants VPN. Ainsi la session de NAT est préservée et le port choisi pour la translation reste toujours le même. La renégociation d'un tunnel en fin de durée de vie peut ainsi être initiée par le répondeur sur le port translaté.

Le paquet UDP se présente de la façon suivante :



KEEPALIVE Header Format

L'entête UDP ci-dessus correspond à un entête standard définit par la RFC 768. Il contient :

► Le port source et le port destination. Ces champs doivent être identiques à ceux utilisés pour l'encapsulation des flux ESP dans l'UDP,

► La somme de contrôle UDP doit être définie à 0,

► Le payload de ce paquet doit être défini à la valeur hexadécimal 0xFF par l'inititateur de la connexion VPN (seul des deux correspondants qui est censé envoyer des KEEPALIVE, bien que dans la pratique certaines solutions permettent au répondeur d'envoyer des KEEPALIVE).

Configuration du NAT-T sur l'appliance UTM NETASQ

Cette fonctionnalité est activée de manière transparente sur les IPS-Firewalls NETASQ. Si le correspondant VPN supporte la fonctionnalité de NAT-T alors elle sera mise en place si besoin est. Si le correspondant VPN ne supporte pas la fonctionnalité de NAT-T alors la fonctionnalité ne sera pas mise en place.

Limitation de la fonctionnalité

La fonctionnalité NAT-T NETASQ ne supporte pas les architectures dans lesquelles on retrouve l'utilisation de plusieurs clients VPN mobile derrière une même adresse IP (donc activation des fonctionnalités NAT-T).

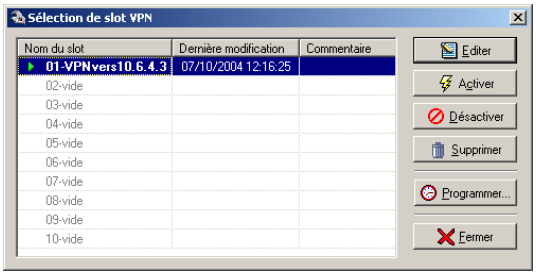
© Copyright NETASQ 2006

VPN IPSEC sur les IPS-Firewalls NETASQ

La configuration des tunnels VPN IPSEC est accessible par le sous menu « Tunnel VPN IPSEC » présent, sous le menu « VPN » de l'arborescence des menus de l'application Firewall Manager. La configuration d'un tunnel VPN IPSEC s'effectue en trois étapes :

1. La sélection d'un slot de politique VPN ;
2. Réalisation des premières étapes de configuration grâce à un assistant ;
3. Fin de la configuration VPN dans le menu de configuration des tunnels VPN IPSEC.

Sélection d'un slot de politique VPN



Lorsque vous sélectionner le sous menu « VPN > Tunnels VPN IPSEC » une boîte de dialogue s'affiche, elle vous permet de manipuler les fichiers de configuration associés aux configurations VPN IPSec.

Elle est découpée en deux zones :

► Gauche : Liste des fichiers de configuration ;
► Droite : Actions sur le fichier sélectionné.

Liste des fichiers de configuration

Dans cette partie de la boîte de dialogue se trouve la liste des fichiers de configuration. Il en existe 10, numérotés de 01 à 10.

Chaque fichier de configuration possède un nom, une date/heure de mise en activité et la date de dernière modification effectuée sur ce fichier de configuration.

L'activation contient l'heure et le/les jours d'activation du fichier. Les jours sont repérés par le numéro du jour dans la semaine (1=lundi). (Voir « Programmation horaire »).

Le fichier de configuration en cours d'activité est indiqué par une petite flèche verte à gauche de son nom.

Un fichier de configuration est dit « en activité » lorsque les paramètres qu'il contient sont en service. Il ne peut y avoir plus d'un fichier de configuration en activité car les paramètres du dernier fichier de configuration activé écrasent ceux du fichier de configuration activé précédemment.

Si vous modifiez un fichier de configuration, vous devez le réactiver pour prendre en compte les modifications. Un fichier de configuration modifié mais non réactivé est notifié par l'icône à la place de la flèche verte habituelle.

© Copyright NETASQ 2006

Il est possible qu'il n'y ait aucun fichier de configuration en activité, cela implique qu'aucun tunnel VPN n'est actif.

Chaque fichier de configuration ne doit pas obligatoirement contenir des paramètres.

Un fichier de configuration pour lequel il n'existe pas de fichier de configuration sur l'IPS-Firewall NETASQ est affiché sous le nom « vide » dans la liste.

Un fichier de configuration est dit sélectionné quand vous faites un simple clic de la souris sur son nom. La sélection faite, vous pouvez l'éditer ou l'activer.

Actions sur le fichier de configuration sélectionné

Quand un fichier de configuration est sélectionné, vous pouvez réaliser différentes actions :

Editer	Modifier la configuration VPN associée à ce fichier de configuration.
Activer	Activer immédiatement un fichier de configuration : les paramètres enregistrés dans ce fichier de configuration écrasent les paramètres en vigueur. Lorsque des modifications sont effectuées sur un slot de politique VPN, une réactivation du slot est nécessaire. Toutefois seul les tunnels impactés par ces modifications seront réactualisés. Ainsi les tunnels VPN pour lesquels aucune modification n'a été effectuée ne sont pas coupés, les connexions ne sont pas coupées.
Programmer	Donner l'heure et le ou les jours auxquels le fichier va s'activer automatiquement.
Effacer	Efface le fichier de configuration et toutes ses informations.
Fermer	Retour à l'écran principal.

Assistant de configuration des tunnels VPN IPSEC

Lorsque le slot de politique choisi est vide, les premières étapes de configuration d'un tunnel VPN IPSEC s'effectue grâce à un assistant de configuration en quatre étapes.

Etape 1

L'étape 1 de la configuration permet de définir le nom qui sera associé à la politique VPN et le modèle de protection qui sera appliqué. Un modèle de type « strong encryption » permettra la mise en place de tunnels VPN IPSEC plus sécurisé (meilleurs algorithmes de chiffrement et d'authentification) qu'un modèle de type « fast encryption ».

Le modèle de protection définit des algorithmes de chiffrement et d'authentification qui peuvent être modifiés dans la suite de la configuration. NETASQ recommande donc de laisser cette option à sa valeur par défaut (à savoir « good encryption ») puis de modifier ce modèle si besoin est.

Etape 2

L'étape 2 de l'assistant est consacrée à la définition du type de tunnel qui est configuré. Trois choix sont proposés. Deux types de tunnels sont basés sur une négociation dynamique des paramètres des tunnels VPN (clé de chiffrement) grâce au protocole IKE, ils différent par le mode d'authentification (clés pré-partagées ou certificats). Notez que le mode « Statique » est obsolète et proposé que par souci d'interopérabilité avec des configurations existantes.

L'option « Mode avancé » est utilisée dans des cas de configuration avancée qui nécessitent l'utilisation de l'objet « any ». Ce type de configuration nécessite une connaissance approfondie du fonctionnement des tunnels VPN IPSEC sur les IPS-Firewalls NETASQ.

Etape 3

L'étape 3 vous demande de définir les extrémités de tunnel. On nomme par extrémités de tunnel, les deux équipements entre lesquels le tunnel est créé et donc les communications chiffrées.

L'interface locale fait référence à l'interface concernée par le tunnel sur votre IPS-Firewall. Par exemple « Firewall_out », interface externe de l'IPS-Firewall ou « Firewall_dialup » si les connexions VPN parviennent à l'IPS-Firewall via un modem configuré dans la partie dialup.

L'interface distant fait référence au correspondant VPN en vis-à-vis de votre IPS-Firewall. Par exemple l'adresse IP publique connue de votre correspondant VPN. Pour les tunnels VPN nomade (l'adresse IP publique n'est pas connue) on choisira l'objet « any », toutefois pour une information complète sur ce type de tunnel veuillez-vous référer aux exemples de configuration.

Etape 4

L'étape 4, quant à elle, vous demande de définir les extrémités de trafic. On nomme par extrémités de trafic, les deux correspondants réels qui vont communiquer au travers du tunnel VPN IPSEC.

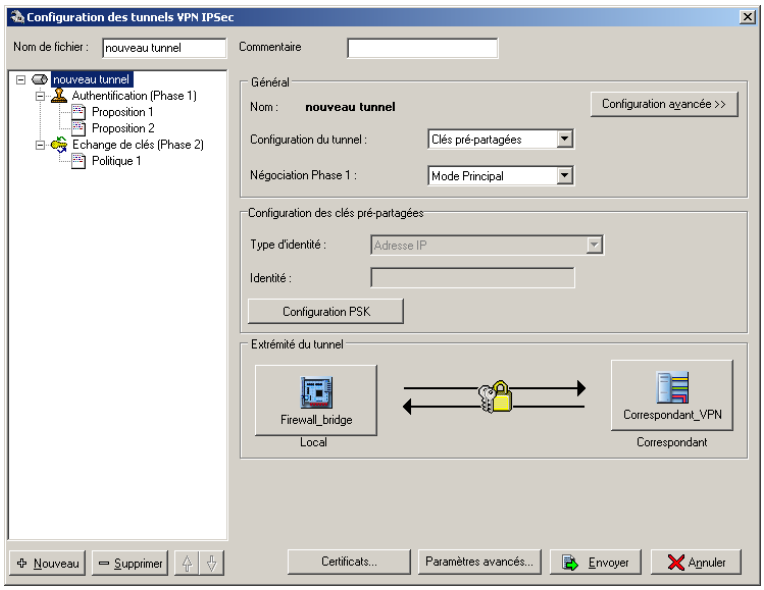
La ou les machines locales font référence aux machines de votre réseau local qui souhaitent communiquer au travers du tunnel VPN. Par exemple « Network_in », votre réseau interne ou « Network_bridge » si vos interfaces internes sont définies en bridge.

La ou les machines distantes font référence aux machines du réseau de votre correspondant VPN. Par exemple l'adresse IP réseau (adresse IP réelle si le réseau distant est translaté). Pour les tunnels VPN nomade (l'adresse IP publique n'est pas connue) on choisira l'objet « any », toutefois pour une information complète sur ce type de tunnel veuillez-vous référer aux exemples de configuration.

Menu de configuration des tunnels VPN

En validant la configuration réalisée grâce à l'assistant, le menu de configuration des tunnels VPN IPSEC apparaît. Celui-ci regroupe l'ensemble des options nécessaires à la création et à la gestion des paramètres d'une politique VPN.

Notez que si vous sélectionnez un slot de VPN non vide, le menu de configuration des tunnels VPN apparaît automatiquement sans nécessiter de suivre une nouvelle fois les étapes de l'assistant. Pour recommencer l'assistant, sélectionnez un slot « vide » ou « supprimez » le slot sélectionné.



Reportez-vous aux sections suivantes pour connaître la signification des différents champs et paramètres.

Lorsqu'un slot de configuration VPN est modifié (ajout d'un nouveau tunnel, suppression ou modification d'un tunnel existant), seuls les tunnels directement concernés par les modifications effectuées sont rechargés lors de la réactivation du slot édité et modifié.

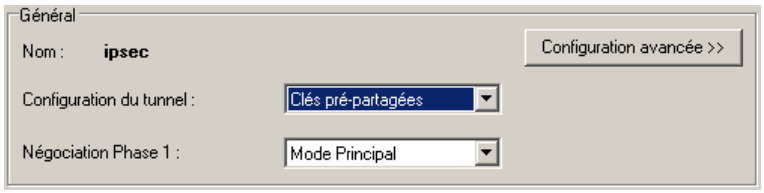
Menu de configuration des tunnels VPN IPSEC

Une politique de tunnels VPN IPSEC est définie par un nom (configuré dans l'assistant de configuration). Ce nom est indiqué en haut du menu de configuration des tunnels VPN IPSEC. Un commentaire peut aussi être ajouté.

Paramètres généraux du tunnel VPN IPSEC

Chaque tunnel VPN IPSEC dans une politique de tunnel VPN IPSEC est aussi défini par son nom. Par défaut ce nom est identique a celui de la politique VPN IPSEC. Cliquez sur le nom du tunnel dans l'arborescence des tunnels configurés pour accéder à l'ensemble des paramètres généraux de ce tunnel.

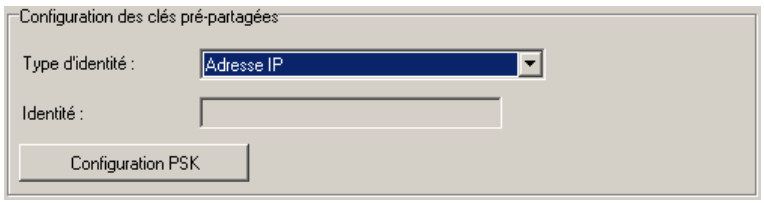
Général



Nom	Le nom du tunnel que vous avez entré au moment de la création du tunnel. Ce nom peut être modifié en cliquant sur le bouton droit de la souris sur le nom du tunnel dans l'arborescence des tunnels configurés.
Configuration du tunnel	Comme dans l'étape 2 cette option définit le type de tunnel VPN IPSEC configuré : par clés pré-partagées, par certificats (PKI) ou par clés manuelles. Les clés manuelles correspondent aux tunnels statiques considérés par NETASQ comme obsolète.
Négociation phase 1	Mode principal : dans ce mode, la phase 1 se déroule en 6 échanges. L'hôte distant ne peut être identifié que par son adresse IP. Ce mode assure l'anonymat. Mode agressif : dans ce mode, la phase 1 se déroule en 3 échanges entre le firewall et l'hôte distant. Ce mode n'assure pas l'anonymat et utilise le certificat comme identifiant. **ATTENTION, l'utilisation du mode agressif + les clés pré-partagées (notamment pour les tunnels VPN à destination de nomades) peut se révéler moins sécuritaire que les autres modes du protocole IPSec. Ainsi NETASQ recommande l'utilisation du mode principal et en particulier du mode principal + certificats pour les tunnels à destination de nomades. En effet la PKI interne de l'IPS-Firewall peut tout à fait fournir les certificats nécessaires à une telle utilisation.** Notez que ce paramètre n'est pas configurable pour les tunnels VPN IPSEC statique.
Configuration avancée	Ce bouton permet l'accès aux options de configuration avancées.

Configuration des clés pré-partagées

Lorsque le type de tunnel VPN IPSEC sélectionné est dynamique par clés pré-partagées, une section de configuration spécifique apparaît. Cette section permet la définition de l'identité locale de votre IPS-Firewall, l'identité du correspondant VPN et la clé partagée par les deux correspondants.



Type d'identité	Le type d'identité permet définir de quelle façon sera identifié votre IPS-Firewall. Il existe trois types d'identité sur un IPS-Firewall NETASQ : l'adresse IP publique, le nom de domaine (FQDN : Full Qualified Domain Name) ou l'adresse Email (user@fqdn). Le mode principal sélectionne automatiquement le type d'identité « Adresse IP ».
Identité	Le champ identité permet définir l'identité de votre IPS-Firewall. Il s'agit de son identité locale. Par exemple firewall@netasq.com dans le cas d'une identité de type « Email ». Le type d'identité « Adresse IP » ne nécessite pas de remplir le champ « identité » car il est automatiquement définit grâce à l'objet choisi pour définir l'extrémité locale de tunnel.

Configuration PSK	Ce bouton permet l'accès aux options de configuration des clés pré-partagées (identité du correspondant distant et clés partagées par les deux correspondants VPN).

Certificats PKI

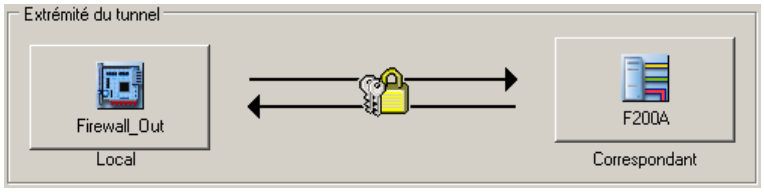
Lorsque le type de tunnel VPN IPSEC sélectionné est dynamique par certificats (PKI), une section de configuration spécifique apparaît. Cette section permet la définition de l'identité locale de votre IPS-Firewall (sous la forme d'un certificat), l'identité du correspondant VPN (sous la forme d'un certificat).

Les certificats utilisés dans la configuration d'un tunnel VPN IPSEC avec authentification par certificat sont configurés dans un menu de configuration des certificats (Voir « Certificats »).

Clé privée	Configuration du certificat de l'IPS-Firewall local (une fenêtre s'ouvre sur la liste des certificats locaux disponibles).
Certificat du correspondant	Configuration optionnelle du certificat de l'IPS-Firewall distant (une fenêtre s'ouvre sur la liste des certificats distants disponibles).

Extrémités de tunnels

Cette section du menu rappelle les extrémités de tunnel configurées dans l'assistant de configuration. Ces extrémités de tunnel peuvent alors être modifiées en cliquant sur les objets représentant les extrémités locales et distante (correspondant) du tunnel.



Local	Interface concernée par le tunnel VPN IPSEC sur l'IPS-Firewall local.
Distant	Adresse IP publique du correspondant VPN distant. Rappel si cette adresse IP n'est pas connue, l'objet « any » doit être utilisé. Reportez-vous aux exemples de configuration avancée de tunnel VPN IPSEC pour plus d'informations sur l'utilisation de l'objet « any ».

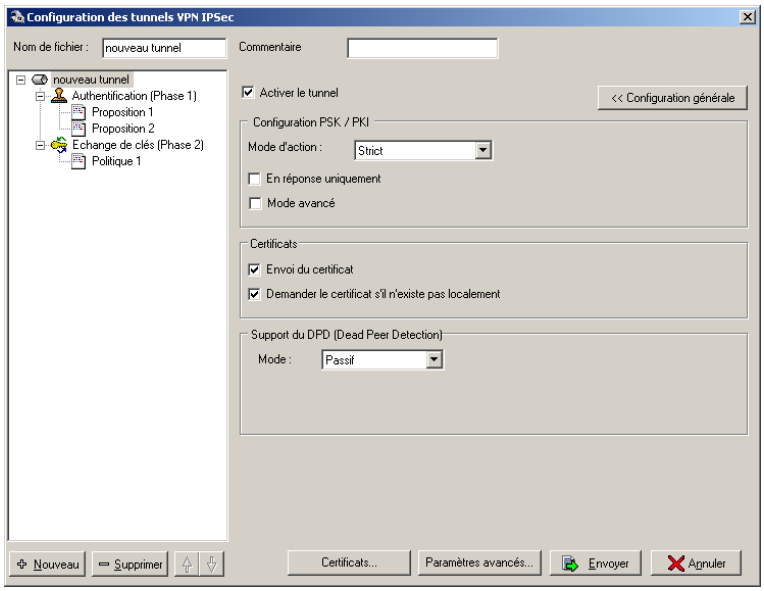
Clés pré-partagées

La configuration des clés pré-partagées permet la définition du secret préalablement échangé entre les deux correspondants du tunnel VPN. Chaque clé pré-partagée est défini en fonction d'un correspondant VPN distant et est OBLIGATOIRE pour des tunnels VPN IPSEC dynamique par clés pré-partagées.

Le menu de configuration des clés pré-partagées est accessible depuis le sous-menu « Clés pré-partagées » du menu « VPN » de l'arborescence du Firewall Manager ou directement dans le menu de configuration des tunnels VPN IPSEC, dans la section « Configuration des clés pré-partagées ».

© Copyright NETASQ 2006

Configuration avancée



Un bouton en haut de la fenêtre, à droite permet de passer en « Configuration avancée ». En configuration avancée, il est possible de modifier :

► le mode d'action,
► l'option « En réponse uniquement »,
► l'option « Mode avancé »,
► Options de la configuration VPN avec Certificats.

Mode d'action

Les modes d'action conditionnent le comportement du serveur IPSEC en phase 1 lors de la négociation des options PFS (Perfect Forward Secrecy) et durée de vie de SA :

► Strict : n'accepte que les options égales ou plus strictes que les siennes (PFS plus élevée, durée de vie de SA plus courte),
► Exact : n'accepte que les options aussi strictes que les siennes (même niveau de PFS, durée de vie de SA strictement égale),
► Obey : accepte les options quelles qu'elles soient (niveau de PFS, durée de vie de SA),
► Claim : accepte que les options égales ou moins strictes que les siennes (PFS moins élevée, durée de vie de SA plus longue) mais choisit toujours les options les plus strictes,

Attention les modes d'action « Obey » et « Claim » ne sont pas couverts par les Critères Communs.

En réponse uniquement

L'option "En réponse uniquement" met le serveur IPSEC en attente. Il ne prendra pas l'initiative de négociation du tunnel. Cette option est utilisée dans le cas d'un client mobile en IP dynamique.

Mode avancé

L'option « mode avancé » permet quant à elle, de pouvoir spécifier <any> aux deux correspondants. Grâce à cette fonctionnalité vous pouvez réaliser un rebond sur un firewall NETASQ pour du Hub'n spoke par exemple.

Attention cette fonction doit être utilisée avec prudence car elle permet la réalisation de configurations potentiellement « erronées ».

Le Hub'n Spoke permet aux machines d'un LAN satellite disposant d'un VBox Agency ou d'un IPS-Firewall NETASQ d'accéder aux LANs des autres sites satellites et/ou à l'extérieur, le tout au travers d'un tunnel avec le site central. Tout le trafic est alors analysé par l'IPS-Firewall NETASQ.

Certificats

Il est possible d'envoyer automatiquement le certificat local au correspondant par l'option « Envoi du Certificat ».

Il est possible de récupérer le certificat du correspondant automatiquement s'il n'existe pas dans la base locale par l'option "Demander le certificat s'il n'existe pas localement".

Support du DPD (Dead Peer Detection)

Ce menu permet de configurer la fonctionnalité VPN dite de Dead Peer Detection. Le DPD permet la renégociation des tunnels mal montés ou mal terminés. Si un tunnel est tombé chez un correspondant VPN nommé « A » celui-ci contacte son vis-à-vis nommé « B » pour renégocier une phase 2 avec celui-ci. Si la négociation échoue le correspondant « A » force la renégociation de toutes les SA (phase 1 et phase 2). Cette fonctionnalité apporte une stabilité au service VPN sur les IPS-Firewalls NETASQ.

Pour configurer l'option de DPD, quatre choix sont disponibles :

► Passif : l'option de DPD est supportée mais l'IPS-Firewall ne prendra pas l'initiative d'établir un tunnel VPN IPSEC avec DPD.

► Fort et Faible : sont deux profils configurés par défaut d'utilisation de l'option DPD. Si le correspondant VPN supporte le DPD, l'IPS-Firewall tentera de négocier les paramètres indiqués.

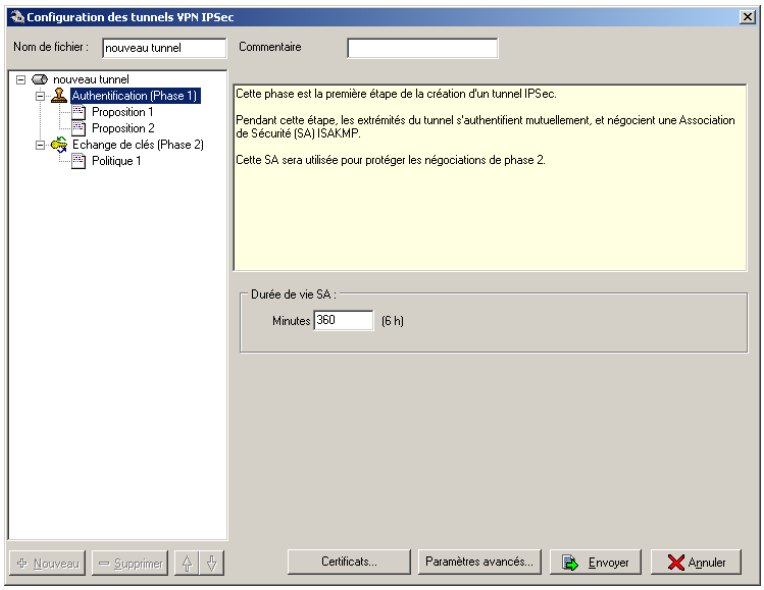
► Manuel : il s'agit de configurer l'option DPD manuellement selon les paramètres suivants :

► Le premier paramètre, « Délai » permet de définir l'intervalle entre chaque envoi de paquet entre les correspondants indiquant que le tunnel est toujours actif.

► Lorsqu'un paquet n'arrive pas à destination (indiquant peut être que le tunnel n'est plus actif), l'intervalle de temps prend la valeur du champ « Essayer à nouveau ».

► La tentative de communication avec le correspondant est ressayée un nombre de fois défini par le champ « nombre d'erreurs maximum ».

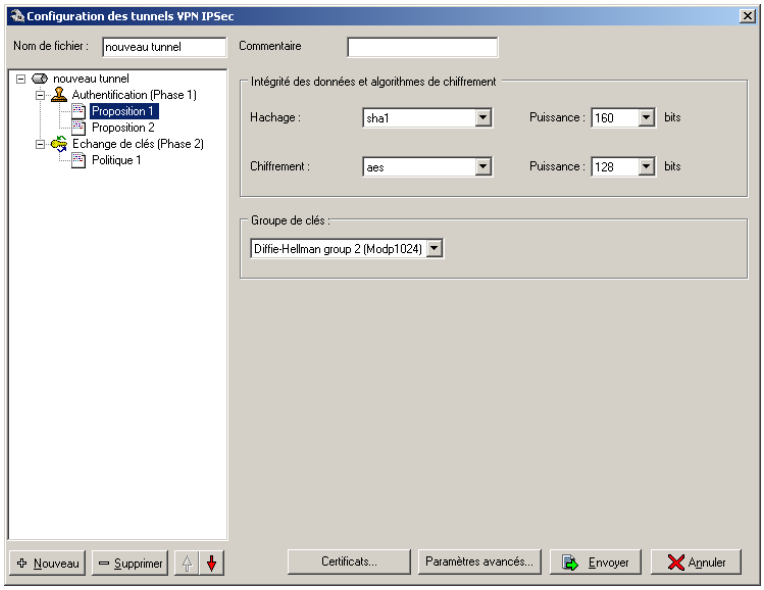
Paramètres généraux de l'authentification [phase 1 IKE]


Configuration des tunnels VPN IPSec
Nom de fichier :
nouveau tunnel
Commentaire
nouveau tunnel
Authentification (Phase 1)
Proposition 1
Proposition 2
Echange de clés (Phase 2)
Politique 1
Cette phase est la première étape de la création d'un tunnel IPSec.
Pendant cette étape, les extrémités du tunnel s'authentifient mutuellement, et négocient une Association de Sécurité (SA) ISAKMP.
Cette SA sera utilisée pour protéger les négociations de phase 2.
Durée de vie SA :
Minutes 360 (6 h)
Nouveau
Supprimer
Certificats...
Paramètres avancés...
Envoyer
Annuler

Les paramètres généraux de la phase 1 sont :

Durée de vie SA	Période de temps ou volume de données au bout desquels les éléments de la phase 1 sont renégociés. Par défaut, le délai est de 360 minutes.

Algorithmes supportés pour la phase 1 de ce tunnel



Les propositions correspondent aux différents algorithmes d'authentification et de chiffrement supportés dans la phase 1 par le firewall pour ce tunnel. Pour qu'un hôte distant puisse établir la phase 1 du protocole IPSEC, il faut qu'au moins une des propositions soit commune avec le firewall.

Vous pouvez établir plusieurs propositions pour un même tunnel.

Les paramètres de la proposition sont :

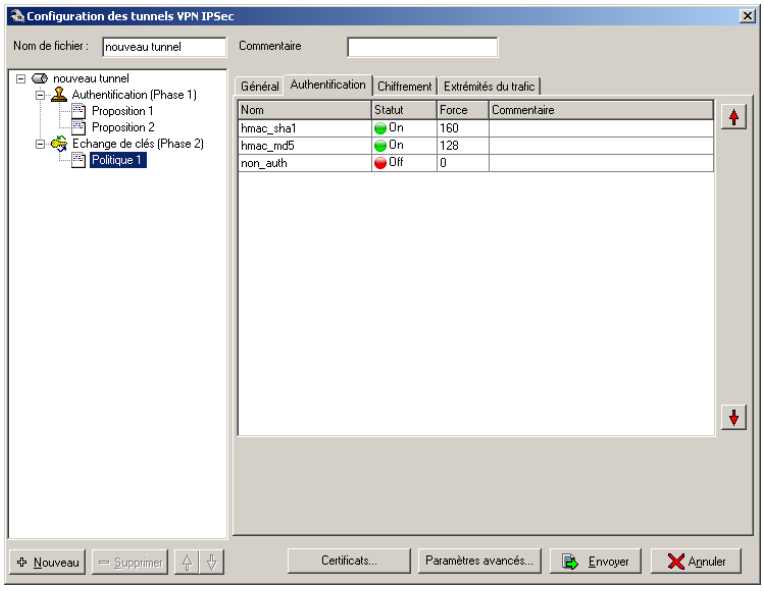
Hachage	Algorithme utilisé pour garantir l'intégrité des données. Les firewalls NETASQ supportent les fonctions de hachage : ► SHA1 (160 bits), ► MD5 (128 bits).
Chiffrement	Algorithme utilisé pour chiffrer les données. Les firewalls NETASQ proposent les algorithmes suivants : ► DES (64 bits), ► 3-DES (192 bits), ► BLOWFISH (40 à 256 bits*), ► CAST128 (40 à 128 bits), ► Rijndael (AES 256 bits*). *selon la législation en vigueur.* **Attention NETASQ recommande vivement l'utilisation de l'AES car c'est l'algorithme le plus performant en terme de débit et aussi le plus sécuritaire. IL FAUT bien comprendre que les algorithmes présentés plus haut ne sont pas égaux en terme de performances et de débit. L'AES est actuellement le meilleur algorithme de chiffrement.**

Groupe de clés	Méthode utilisée pour le calcul des clés. En mode agressif, cette méthode est commune à toutes les propositions et est choisie dans les paramètres généraux de la phase 1.

Paramètres généraux de l'échange des clés [phase 2 IKE]

Méthode de proposition	Sélection des protocoles IPSec utilisés dans le tunnel : ► protocole AH (authentification) ► protocole ESP (chiffrage) ► protocole AH et ESP.
Maintenir la connexion	Temps écoulé, en secondes, entre deux paquets envoyés au travers d'un tunnel VPN pour assurer le maintien de ce tunnel. Les paquets envoyés sont uniquement utilisé pour le maintien de connexion.
Perfect Forward Secrecy	Permet de garantir qu'il n'y a aucun lien entre les différentes clés de chaque session. Les clés sont re-calculées par l'algorithme de Diffie-Hellman sélectionné. Plus le chiffre est élevé (aucune, 1, 2 ou 5), plus la sécurité est importante. 2 est le niveau de PFS le plus couramment utilisé.
Vie de SA	Période de temps ou volume de données au bout desquels les clés sont renégociées. La période est par défaut de 60 minutes.

Onglet Authentification

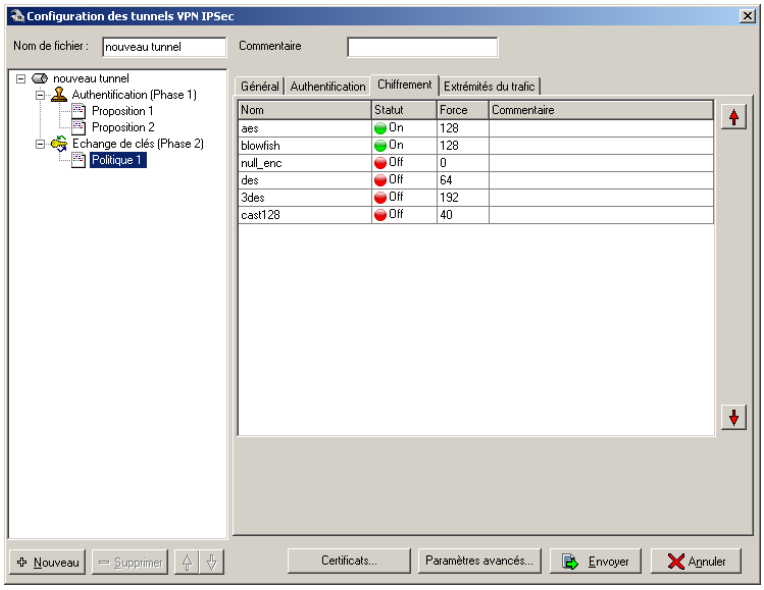


L'onglet « Authentification » vous permet de sélectionner les algorithmes d'authentification acceptés par cette proposition.

L'IPS-Firewall supporte les algorithmes suivants :

► pas d'authentification,
► HMAC-SHA1,
► HMAC-MD5.

Onglet Chiffrement


Configuration des tunnels VPN IPSec
Nom de fichier : nouveau tunnel
Commentaire
nouveau tunnel
Authentification (Phase 1)
Proposition 1
Proposition 2
Echange de clés (Phase 2)
Politique 1
Général | Authentification | Chiffrement | Extrémités du trafic
Nom | Statut | Force | Commentaire
aes | On | 128
blowfish | On | 128
null_enc | Off | 0
des | Off | 64
3des | Off | 192
cast128 | Off | 40
Nouveau | Supprimer | Certificats... | Paramètres avancés... | Envoyer | Annuler

L'onglet « Chiffrement » vous permet de sélectionner les algorithmes de chiffrement acceptés par cette proposition.

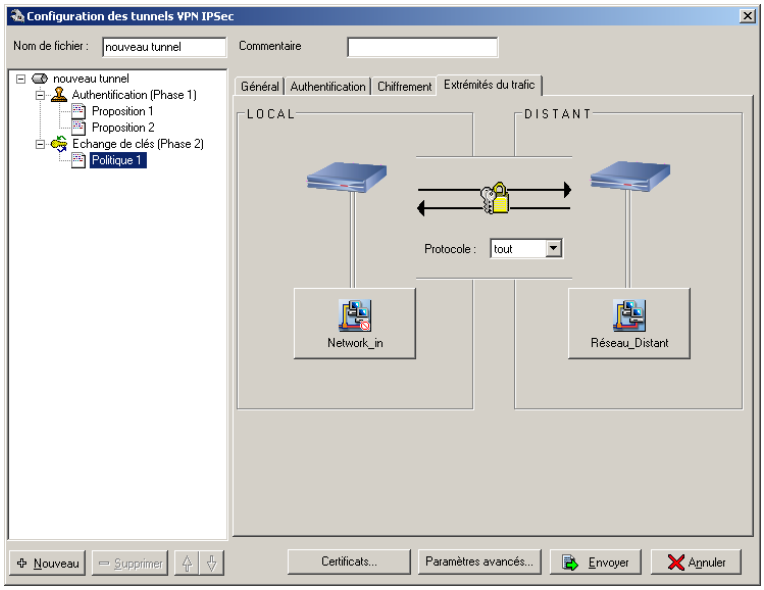
L'IPS-Firewall supporte les algorithmes suivants :

- ► pas de chiffrement,
- ► DES (64 bits),
- ► 3-DES (192 bits),
- ► BLOWFISH (40 à 256 bits*),
- ► CAST128 (40 à 128 bits),
- ► Rijndael (AES 256 bits*).

selon la législation en vigueur.

Attention NETASQ recommande vivement l'utilisation de l'AES car c'est l'algorithme le plus performant en terme de débit et aussi le plus sécuritaire. IL FAUT bien comprendre que les algorithmes présentés plus haut ne sont pas égaux en terme de performances et de débit. L'AES est actuellement le meilleur algorithme de chiffrement.

Onglet Extrémités du trafic



Cette section vous permet de définir quels utilisateurs locaux utilisent le tunnel et éventuellement pour quels protocoles.

Notez l'utilisation particulière de l'objet « any » en extrémité de trafic distante. Cet objet définit que l'on prévoit de pouvoir communiquer avec TOUT réseau distant. De ce cas précis, il faut faire la différence entre « tout » et « n'importe quel » réseau (ou machine) distant. Cela signifie que si l'on utilise l'objet « any » en extrémité de trafic distante, il DOIT être retrouvé dans la configuration de la politique VPN du site distant (on ne peut pas y trouver « n'importe quel » réseau). L'utilisation de l'objet « any » provient essentiellement de l'utilisation du VPN dans une configuration dite de Hub'n Spoke (reportez vous à la note technique sur le Hub'n Spoke disponible sur le site Web NETASQ).

Vous sélectionnez les machines distantes dans la liste des objets déclarés puis éventuellement un protocole particulier à chiffrer.

Paramètres avancés

Ce menu vous permet de gérer des paramètres supplémentaires pour un tunnel IPSEC. Il est disponible autant pour les tunnels statiques que pour les tunnels dynamiques, en cliquant sur le bouton "paramètres avancés" de la fenêtre de configuration des tunnels VPN.

C'est ici que l'on va mettre en place le comportement général du tunnel sélectionné.

Considérer les correspondants IPSEC comme internes

En cochant cette option, les Interfaces IPSEC sont considérées comme interfaces internes. Donc cela leur confère un caractère « protégé » comme toutes interfaces internes. Cette option est notamment nécessaire pour la configuration du Hub'n spoke.

Utiliser la SA la plus ancienne

L'option permet de remonter un tunnel si une extrémité tombe et tente de renégocier. Si elle ne peut plus remonter le tunnel.

Si cette option est décochée, on va utiliser immédiatement la nouvelle clé lors d'une nouvelle négociation sans atteindre la fin de durée de vie de l'ancienne SA.

Pour utiliser une SA jusqu'à la fin de sa durée de vie, il suffit de cocher cette option.

Il est conseillé d'activer cette option.

Faire confiance à la PKI interne

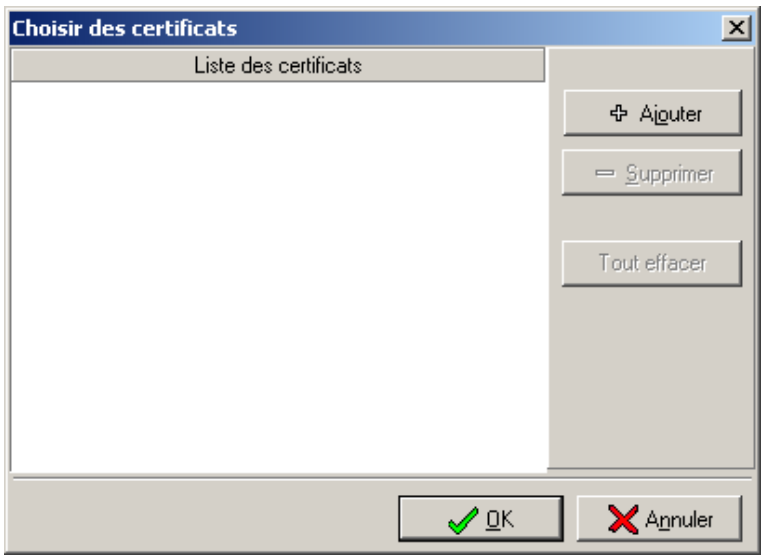
Lorsque vous utilisez un tunnel VPN utilisant des certificats numériques et que vous cochez cette option, tout correspondant dont le certificat appartient à la PKI interne et qui n'est pas révoqué par la CRL interne sera accepté.

Tester la CRL interne

Cochez cette option afin de paramétrer la fréquence de mise à jour de la liste de révocation des certificats (CRL). Il est possible de faire des vérifications régulières, pour cela, paramétrez la base de temps (en minutes, heures, jours ou mois).

Plus le délai est court, plus le firewall devra vérifier sa CRL lorsque ce tunnel est actif. Donc il vaut mieux ne pas définir un temps trop court (baisse de performances), ni trop long (risque d'utiliser une CRL obsolète).

Certificats



Lorsque des certificats d'autorité de certification externe sont insérés dans la liste des certificats externes, tous les certificats utilisateurs signés par ces autorités de certification sont automatiquement reconnus par l'IPS-Firewall comme certificat valide à l'authentification de leur détenteur.

Pour utiliser ces autorités de certification reconnues, dans la configuration des politiques VPN, il faut spécifier dans le menu « Certificat » du panneau de configuration générale des tunnels VPN, la liste des autorités de certification qui doivent être validées pour ce slot de configuration VPN. Cette liste d'autorité de certification est spécifique au slot configurée bien que l'on retrouve la liste globale de toutes les autorités de certification autorisée par l'administrateur dans un seul et même endroit, le menu de configuration des Certificats de l'arborescence des menus du Firewall Manager.

Pour ajouter une autorité de certification dans la liste des autorités reconnues pour le slot VPN configuré, reportez-vous à la procédure suivante :

1. Cliquez sur le bouton « Certificat » du panneau de configuration générale des tunnels VPN ;

2. Cliquez sur le bouton « Ajouter » du panneau de configuration des certificats ;

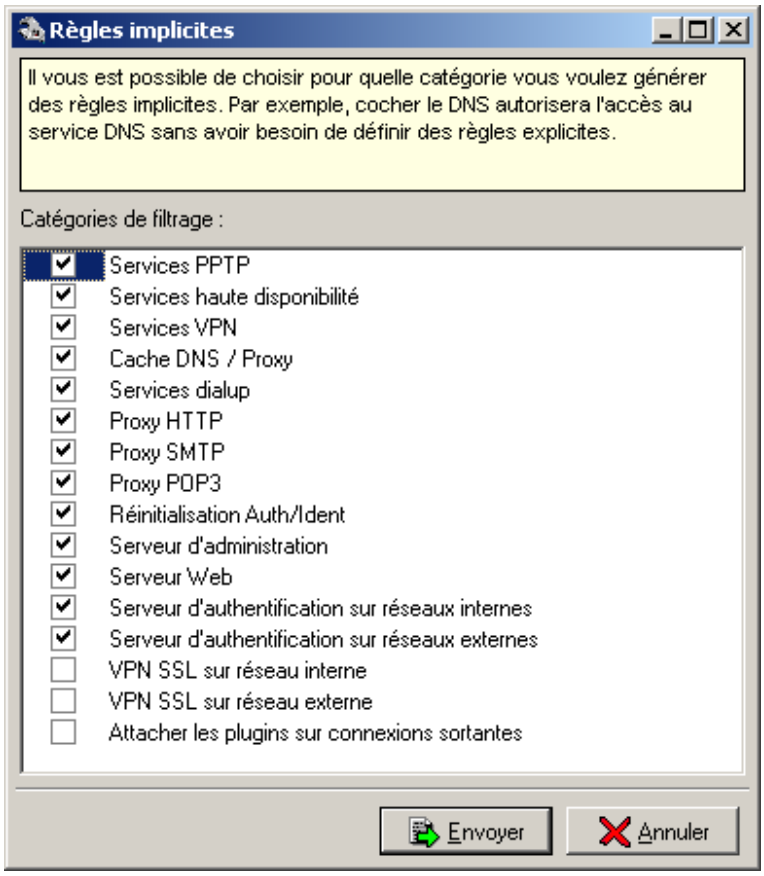
3. Sélectionnez les certificats d'autorité de certification qui doivent être utilisées pour ce slot de configuration VPN ;

4. Validez enfin l'ajout de ces certificats en envoyant la configuration du slot VPN.

Après la configuration du ou des tunnels VPN, il faut définir un ensemble de règles de filtrage permettant l'établissement du ou des tunnels et la transmission des informations chiffrées. Pour cela, deux actions doivent être réalisées :

► activation des règles implicites VPN,
► édition des règles de filtrage pour autoriser le trafic au travers d'un tunnel IPSEC.

Activation des règles implicites VPN


Règles implicites
Il vous est possible de choisir pour quelle catégorie vous voulez générer des règles implicites. Par exemple, cocher le DNS autorisera l'accès au service DNS sans avoir besoin de définir des règles explicites.
Catégories de filtrage :
Services PPTP
Services haute disponibilité
Services VPN
Cache DNS / Proxy
Services dialup
Proxy HTTP
Proxy SMTP
Proxy POP3
Réinitialisation Auth/Ident
Serveur d'administration
Serveur Web
Serveur d'authentification sur réseaux internes
Serveur d'authentification sur réseaux externes
VPN SSL sur réseau interne
VPN SSL sur réseau externe
Attacher les plugins sur connexions sortantes
Envoyer
Annuler

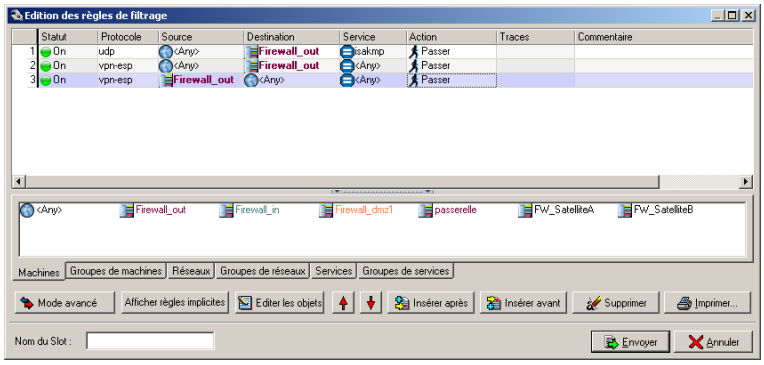
Les IPS-Firewalls NETASQ peuvent générer de façon automatique des règles de filtrage pour l'établissement des tunnels VPN. Ces règles n'ont donc pas besoin d'être définies de façon explicite par l'administrateur au niveau de l'édition des slots de filtrage. L'activation des règles implicites se fait au moyen du menu « Politiques > Règles implicites ».

Activez la case « Services VPN » puis cliquez sur « OK ».

Attention, les règles implicites ne sont générées que pour les tunnels IPSEC Gateway to Gateway. Pour le tunnel anonyme, il faut obligatoirement définir explicitement des règles au niveau des slots de filtrage.

Pour un tunnel anonyme, les règles à définir sont du type :

© Copyright NETASQ 2006



Dans cet exemple, on ne connaît pas la plage d'adresses utilisée par les clients VPN nomades (on utilise donc l'objet "ANY"). Si la plage d'adresses utilisée par les clients nomades est connue (plage d'adresses du fournisseur d'accès, par exemple), alors il est conseillé de restreindre les règles à cette plage d'adresses.

Edition des règles de filtrage

Sans règles de filtrage explicites pour le trafic transitant au travers du tunnel IPSEC, aucune donnée ne sera autorisée au travers de ce tunnel (même si le tunnel est déjà actif). Pour autoriser des données à transiter au travers du firewall, il faut rajouter des règles de filtrage comme dans l'exemple suivant :

	Statut	Interface	Protocole	Message	Source	Port source	Destination	Port destination	Action
1	On	IPSec	group		Netwk_SatelliteA	<Any>	Network_bridge	web	Passer
2	On	auto	all		Network_bridge	<Any>	Netwk_SatelliteA	<Any>	Passer

Dans cet exemple, les machines du réseau distant (Netwk_SatelliteA) ont accès aux machines du réseau interne (Network_bridge) pour les services WEB. Les machines du réseau interne (Network_bridge) ont accès à toutes les machines du réseau distant (Netwk_SatelliteA) pour tous les services.

Attention, les règles de filtrage s'appliquant au trafic venant du réseau distant doivent avoir l'interface « IPSEC » sélectionnée. Les règles de filtrage s'appliquant au trafic en direction du réseau distant doivent avoir l'interface « Auto » sélectionnée.

© Copyright NETASQ 2006

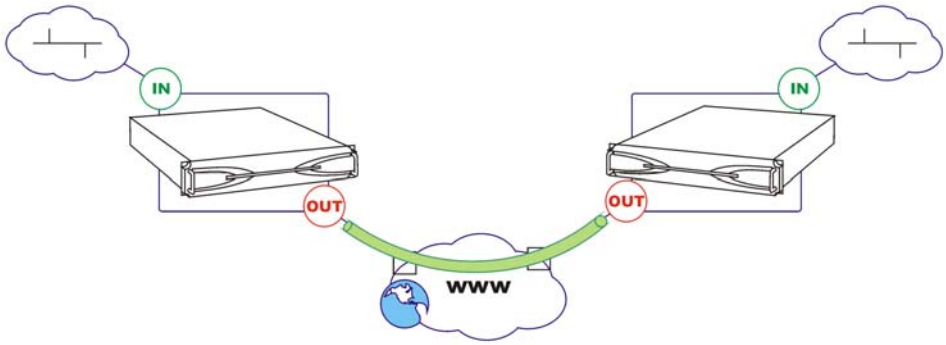
Dans cette section, plusieurs configurations basiques de tunnels VPN sont abordées. Elle décrit en particulier :

► la création d'un tunnel G2G avec clés pré partagées,
► la création d'un tunnel G2G avec certificats,
► la création d'un tunnel G2G VPN statique (ce type de configuration, aujourd'hui obsolète, est uniquement supportée pour des raisons de compatibilités).

Tunnel VPN IPSEC avec clés pré partagées

L'exemple suivant explique la configuration nécessaire à la réalisation d'un tunnel VPN passerelle à passerelle (gateway to gateway dans la littérature anglophone) avec clés pré partagées. On appelle « tunnel VPN passerelle à passerelle » un tunnel VPN réalisé entre deux éléments réseaux compatibles VPN qui jouent le rôle d'extrémités de tunnel, d'une passerelle (essentiellement IPS-Firewall à IPS-Firewall).

Cette architecture est représentée par le schéma suivant :



Configuration du tunnel

Afin de réaliser la configuration du tunnel, sélectionner le slot VPN dans lequel vous désirez réaliser le tunnel. L'assistant VPN vous aiguille alors dans la configuration VPN.

Cette configuration est à réaliser sur chacun des IPS-Firewalls participant au tunnel VPN. Pensez toutefois à inverser les extrémités de trafic et de tunnel.

Le premier écran de l'assistant VPN apparaît. Choisissez le nom que vous désirez attribuer à ce tunnel (le nom du slot sera automatiquement attribué avec cette valeur mais vous pouvez la modifier ensuite). Cliquez sur « suivant » pour continuer la configuration.

A l'étape 2 de l'assistant VPN, choisissez le type de tunnel que vous désirez réaliser (ici dynamique avec clés pré partagées pour l'exemple). Cliquez sur « suivant ».

Les étapes 3 et 4 permettent de spécifier dans un premier temps les différents éléments réseaux aux extrémités du tunnel puis les extrémités du trafic transitant à l'intérieur du tunnel VPN.

Attention, dans l'exemple l'interface Firewall_out est utilisée comme extrémité de tunnel. Si votre IPS-Firewall est directement relié à un modem vous devez utiliser l'interface Dialup qui correspond à votre connexion Internet active.

© Copyright NETASQ 2006

Lorsque les extrémités sont définies, cliquez sur suivant pour terminer la configuration du tunnel. Un écran général rappelle la configuration définie dans l'assistant. Vous pouvez contrôler cette configuration avant d'envoyer la configuration VPN spécifiée à l'IPS-Firewall.

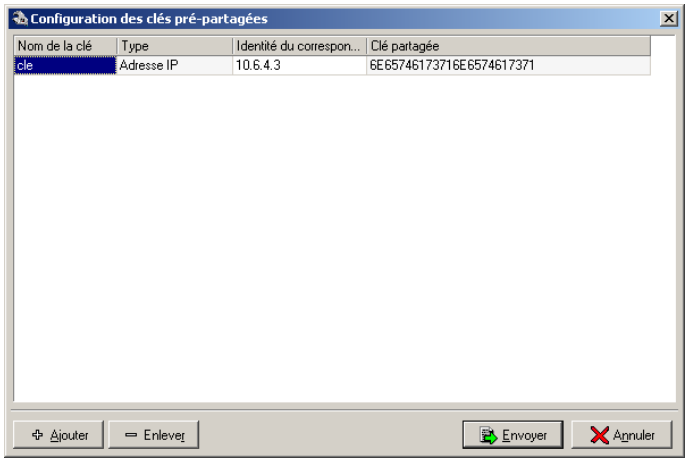
Attention pour qu'un tunnel VPN soit négocié il est nécessaire qu'il possède une passerelle par défaut valide (même lors d'une phase de test).

Pensez à effectuer le filtrage nécessaire au passage du trafic VPN sur les IPS-Firewalls participant au tunnel.

Configuration des clés pré partagées

Suite à la configuration du tunnel il convient de configurer les clés pré partagées. Cette configuration est réalisée dans le menu « VPN > Clés pré partagées » et grâce au bouton « Configuration des clés pré partagées » du menu général de configuration du VPN.

Remarque : les clés pré-partagées pour les clients mobiles peuvent aussi être indiquées directement dans les fiches des utilisateurs (voir section « Configuration des objets > utilisateurs »). Dans ce cas, chaque utilisateur aura sa propre clé pré partagée pour s'authentifier auprès de l'IPS-Firewall lors d'un accès distant via VPN.



Nom de la clé	Nom que vous affectez à cette clé. Valable uniquement pour l'utilisation interne de l'IPS-Firewall.
Type	Type d'identifiant de la machine distante. Les différentes possibilités sont : ► Adresse IP : la machine distante est identifiée par son adresse IP, ► Fqdn (Full qualified domain name) : nom de domaine de la machine (ex : firewall.netasq.com), ► User@Fqdn : nom de la machine sur un domaine. Il n'y a pas de lien effectué avec un domaine. L'identifiant doit juste être le même sur la machine distante.
Identité	Identifiant de la machine distante en fonction du type préalablement sélectionné.
Clé pré-partagée	Valeur de la clé en hexadécimal par défaut.

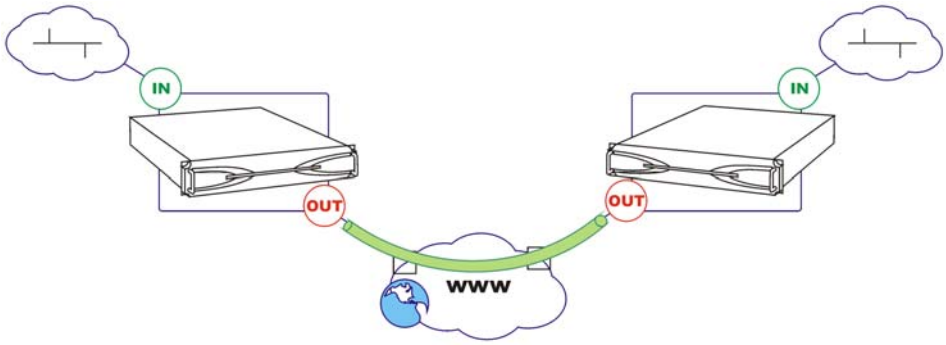
Lors du mode principal la seule identité disponible pour ce tunnel est l'adresse IP.

Les clés ne sont pas liées à une machine (sauf avec l'identité de type adresse IP) et peuvent être utilisées par plusieurs utilisateurs en même temps.

Tunnel VPN IPSEC avec certificats

L'exemple suivant explique la configuration nécessaire à la réalisation d'un tunnel VPN passerelle à passerelle (gateway to gateway dans la littérature anglophone) avec certificats. On appelle « tunnel VPN passerelle à passerelle » un tunnel VPN réalisé entre deux éléments réseaux compatibles VPN qui jouent le rôle d'extrémités de tunnel, d'une passerelle (essentiellement IPS-Firewall à IPS-Firewall).

Cette architecture est représentée par le schéma suivant :



Configuration du tunnel

Afin de réaliser la configuration du tunnel, sélectionner le slot VPN dans lequel vous désirez réaliser le tunnel. L'assistant VPN vous aiguille alors dans la configuration VPN.

Cette configuration est à réaliser sur chacun des IPS-Firewalls participant au tunnel VPN. Pensez toutefois à inverser les extrémités de trafic et de tunnel.

La première étape dans la création du tunnel est de choisir le nom que vous désirez attribuer à ce tunnel (le nom du slot sera automatiquement attribué avec cette valeur mais vous pouvez la modifier ensuite). Cliquez sur « suivant » pour continuer la configuration.

A l'étape 2 de l'assistant VPN, choisissez le type de tunnel que vous désirez réaliser (ici dynamique avec certificats pour l'exemple). Cliquez sur « suivant ».

Les étapes 3 et 4 permettent de spécifier dans un premier temps les différents éléments réseaux aux extrémités du tunnel puis les extrémités du trafic transitant à l'intérieur du tunnel VPN.

Attention, dans l'exemple l'interface Firewall_out est utilisée comme extrémité de tunnel. Si votre IPS-Firewall est directement relié à un modem vous devez utiliser l'interface Dialup qui correspond à votre connexion Internet active.

Lorsque les extrémités sont définies, cliquez sur suivant pour terminer la configuration du tunnel. Un écran général rappelle la configuration définie dans l'assistant.

Attention pour qu'un tunnel VPN soit négocié il est nécessaire qu'il possède une passerelle par défaut valide (même lors d'une phase de test).

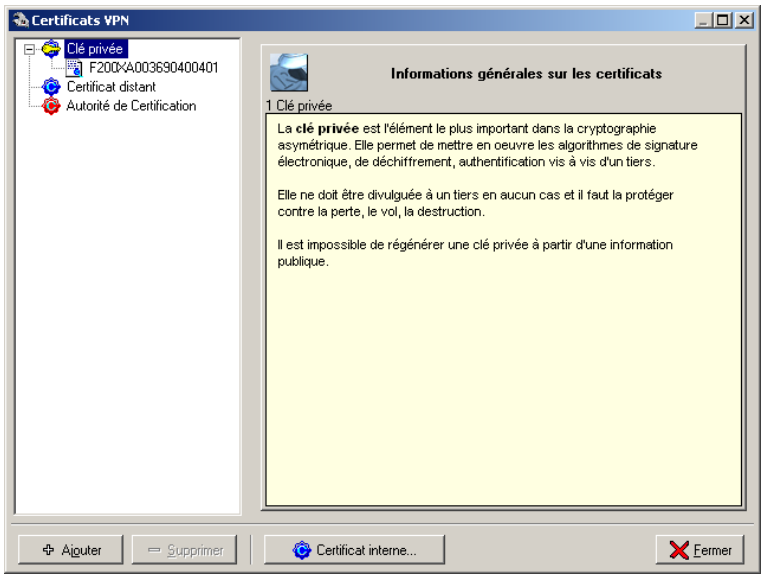
Pensez à effectuer le filtrage nécessaire au passage du trafic VPN sur les IPS-Firewalls participant au tunnel.

Configuration des certificats

Suite à la configuration du tunnel, il convient de configurer les certificats. Dans le cadre « Certificats PKI » de l'écran de configuration globale des tunnels VPN, cliquez sur le bouton situé en face de l'option « Clé privée ».

Vous pouvez alors générer un certificat numérique pour l'IPS-Firewall. Pour cela, cliquez sur le bouton « certificat VPN » puis indiquez le mot de passe de l'autorité de certification de l'IPS-Firewall. Une fois généré, le certificat apparaît dans la partie "Clé privée".

Un seul certificat peut être généré.


Certificats VPN
Clé privée
F200XA003690400401
Certificat distant
Autorité de Certification
Informations générales sur les certificats
1 Clé privée
La clé privée est l'élément le plus important dans la cryptographie asymétrique. Elle permet de mettre en oeuvre les algorithmes de signature électronique, de déchiffrement, authentification vis à vis d'un tiers.
Elle ne doit être divulguée à un tiers en aucun cas et il faut la protéger contre la perte, le vol, la destruction.
Il est impossible de régénérer une clé privée à partir d'une information publique.
Ajouter
Supprimer
Certificat interne...
Fermer

Attention la génération de certificats n'est disponible que dans le cas où le service PKI interne est configuré et actif sur l'IPS-Firewall.

Configuration avancée avec les certificats

Si le correspondant est un client mobile, vous pouvez définir son certificat dans la fiche de l'utilisateur utilisant le client IPSEC. (Voir section « Configuration des objets > utilisateurs »).

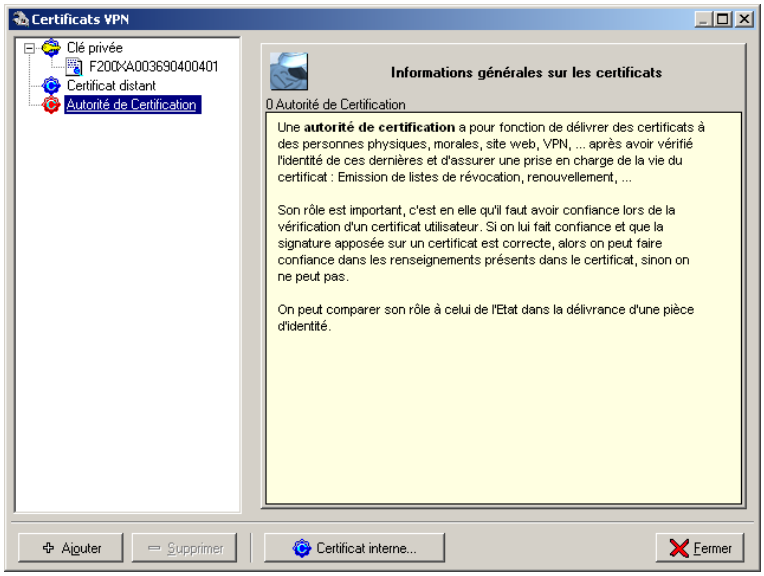
Si le correspondant est une autre passerelle VPN :

► Vous pouvez exporter votre autorité de certification interne dans l'autre firewall (voir la section « Configuration de l'authentification ») et importer l'autorité de certification du firewall distant dans la partie « Autorité de certification » (de façon croisée).

► Vous pouvez définir l'IPS-Firewall distant comme un utilisateur. Dans ce cas, vous devez ajouter une fiche utilisateur (Voir section « Configuration des objets > utilisateurs ») pour l'IPS-Firewall distant et générer le certificat. Vous devez sauvegarder ce certificat et l'importer dans la partie « Clés privées et certificats » de l'IPS-Firewall distant.

Intégration de l'architecture VPN dans une PKI externe

L'IPS-Firewall NETASQ peut intégrer les certificats provenant d'une PKI externe. Les certificats doivent alors être importés au niveau de l'IPS-Firewall. Dans la fenêtre Certificats VPN, avant l'importation, la fenêtre ne contient que le certificat de l'IPS-Firewall.


Certificats VPN
Clé privée
F200XA003690400401
Certificat distant
Autorité de Certification
Informations générales sur les certificats
0 Autorité de Certification
Une autorité de certification a pour fonction de délivrer des certificats à des personnes physiques, morales, site web, VPN, ... après avoir vérifié l'identité de ces dernières et d'assurer une prise en charge de la vie du certificat : Emission de listes de révocation, renouvellement, ...
Son rôle est important, c'est en elle qu'il faut avoir confiance lors de la vérification d'un certificat utilisateur. Si on lui fait confiance et que la signature apposée sur un certificat est correcte, alors on peut faire confiance dans les renseignements présents dans le certificat, sinon on ne peut pas.
On peut comparer son rôle à celui de l'Etat dans la délivrance d'une pièce d'identité.
Ajouter
Supprimer
Certificat interne...
Fermer

La colonne de gauche affiche trois types de certificats. Lorsque vous sélectionnez un type de certificat une explication sur le type de clé sélectionné apparaît.

Pour ajouter un certificat provenant d'une PKI externe, reportez-vous à la procédure suivante :

1. Cliquez sur le bouton « Ajouter », un assistant d'intégration des certificats apparaît, la première étape permet de saisir le nom du certificat, continuer l'assistant,

2. La deuxième étape permet de choisir le type de certificat,

3. La troisième étape permet de sélectionner le fichier certificat que l'on désire insérer.

Suivant le type de certificat, l'assistant d'intégration des certificats requiert des fichiers différents à la troisième étape.

► Le choix « Clés privées et certificats » donne la possibilité de charger le certificat (au format *.cer, *.der ou *.pem) et la clé privée (au format *.key ou *.pem non chiffré c'est à dire texte clair) dans deux fichiers différents.

Le firewall teste si le certificat correspond bien à la clé privée.

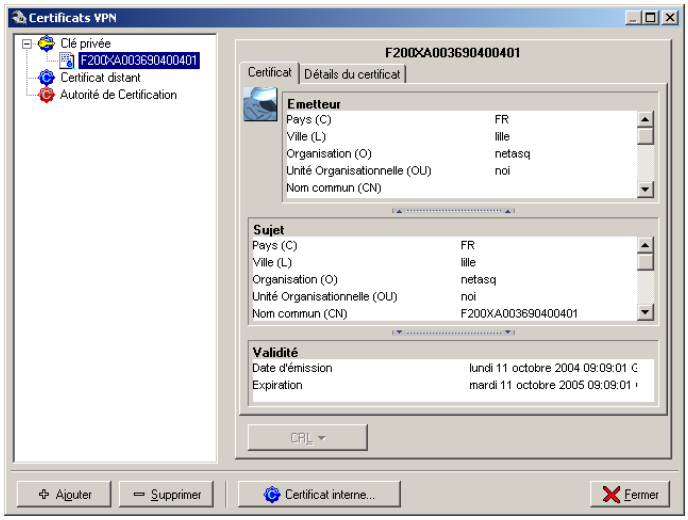
► Le choix « Certificats des correspondants » donne la possibilité de charger le certificat (au format *.cer, *.der ou *.pem) :

► Le choix « Autorités de certification » donne la possibilité de charger le certificat (au format *.cer, *.der ou *.pem) ainsi que la liste de révocation des certificats (au format *.crl ou *.pem) :

La liste de révocation des certificats est une option. Toutefois une fois un premier fichier configuré, il faut mettre à jour la liste dès que celle-ci est périmée. Dans le cas contraire, l'autorité de certification sera inutilisable.

► Le choix « Container PKS#12 » donne la possibilité de charger un fichier PKCS#12. Un container PKCS#12 contient une clé privée, une clé publique et un certificat. Toutes ces informations sont chiffrées en utilisant un mot de passe qu'il faut préciser.

Le contenu et le détail du certificat peut être visualisé dans la partie droite de la fenêtre grâce aux onglets « Certificat » et « Détails du certificat ».



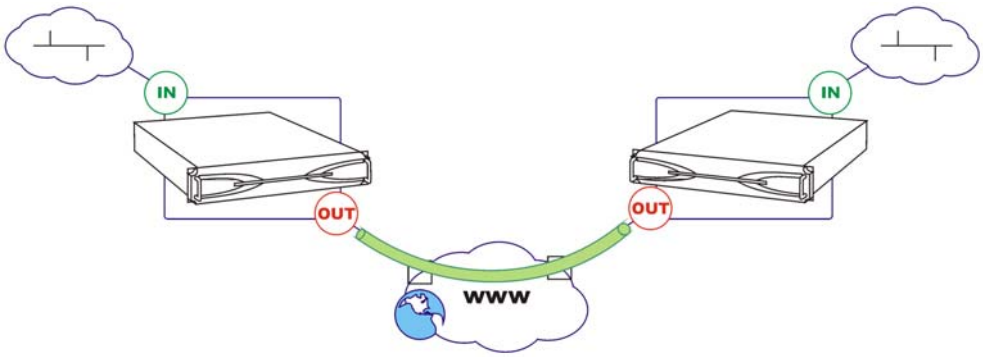
Nota : on y retrouve entre autres le propriétaire du certificat, l'autorité de certification qui a signé le certificat, la période de validité du certificat. Le certificat devient grisé s'il n'est plus valide.

Lorsqu'une autorité de certification externe est insérée dans le menu certificat, tous les certificats signés par cette autorité de certification sont automatiquement reconnus comme certificats valides à l'authentification de leur détenteur.

Tunnel VPN IPSEC statique

L'exemple suivant explique la configuration nécessaire à la réalisation d'un tunnel VPN passerelle à passerelle (gateway to gateway dans la littérature anglophone) avec clés pré partagées. On appelle « tunnel VPN passerelle à passerelle » un tunnel VPN réalisé entre deux éléments réseaux compatibles VPN qui jouent le rôle d'extrémités de tunnel, d'une passerelle (essentiellement IPS-Firewall à IPS-Firewall).

Cette architecture est représentée par le schéma suivant :



Configuration du tunnel

Afin de réaliser la configuration du tunnel, sélectionner le slot VPN dans lequel vous désirez réaliser le tunnel. L'assistant VPN vous aiguille alors dans la configuration VPN.

Cette configuration est à réaliser sur chacun des IPS-Firewalls participant au tunnel VPN. Pensez toutefois à inverser les extrémités de trafic et de tunnel.

Les première étape de l'assistant de création des tunnels VPN est de choisir le nom que vous désirez attribuer à ce tunnel (le nom du slot sera automatiquement attribué avec cette valeur mais vous pouvez la modifier ensuite). Cliquez sur « suivant » pour continuer la configuration.

A l'étape 2 de l'assistant VPN, choisissez le type de tunnel que vous désirez réaliser (ici tunnel statique). Un message vous prévient qu'il s'agit d'une configuration désormais obsolète. Cliquez sur « suivant ».

Les étapes 3 et 4 permettent de spécifier dans un premier temps les différents éléments réseaux aux extrémités du tunnel puis les extrémités du trafic transitant à l'intérieur du tunnel VPN.

Attention, dans l'exemple l'interface Firewall_out est utilisée comme extrémité de tunnel. Si votre IPS-Firewall est directement relié à un modem vous devez utiliser l'interface Dialup qui correspond à votre connexion Internet active.

Lorsque les extrémités sont définies, cliquez sur « Suivant » pour terminer la configuration du tunnel. Un écran général rappelle la configuration définie dans l'assistant.

Attention pour qu'un tunnel VPN soit négocié il est nécessaire qu'il possède une passerelle par défaut valide (même lors d'une phase de test).

Pensez à effectuer le filtrage nécessaire au passage du trafic VPN sur les IPS-Firewalls participant au tunnel.

Configuration des clés manuelles

Afin de compléter la configuration des tunnels VPN Statique, sélectionner la politique 1 pour accéder du menu de configuration des clés manuelles.

Dans la partie générale de la configuration, vous configurez les paramètres suivants :

Méthode de proposition	Cette option non modifiable indique que le protocole utilisé pour ce tunnel est le protocole ESP en mode tunnel.
Authentification	Algorithme utilisé pour garantir l'intégrité des données. Les firewalls NETASQ supportent les fonctions de hachage : ► Pas d'authentification, ► HMAC-SHA1 (160 bits), ► HMAC-MD5 (128 bits). Vous configurez la clé statique correspondante en cliquant sur l'icône en forme de clé.
Chiffrement	Algorithme utilisé pour chiffrer les données. Les IPS-Firewalls NETASQ proposent les algorithmes suivants : ► Pas de chiffrement, ► DES (64 bits), ► 3-DES (192 bits), ► BLOWFISH (40 à 256 bits*), ► CAST128 (40 à 128 bits), ► Rijndael (AES 256 bits*). *selon la législation en vigueur.*

	Attention NETASQ recommande vivement l'utilisation de l'AES car c'est l'algorithme le plus performant en terme de débit et aussi le plus sécuritaire. IL FAUT bien comprendre que les algorithmes présentés plus haut ne sont pas égaux en terme de performances et de débit. L'AES est actuellement le meilleur algorithme de chiffrement. Vous configurez la clé statique correspondante en cliquant sur l'icône en forme de clé.
SPI (données entrantes)	Identifiant du tunnel entrant. Valeur unique calculée par défaut par l'IPS-Firewall.
SPI (données sortantes)	Identifiant du tunnel sortant. Valeur unique calculée par défaut par l'IPS-Firewall.
Maintenir la connexion	Temps écoulé, en secondes, entre deux paquets envoyés au travers d'un tunnel VPN pour assurer le maintien de ce tunnel. Les paquets envoyés sont uniquement utilisé pour le maintien de connexion.

Remarque: Les valeurs des SPI doivent être inversées (entrant et sortant) dans la configuration du tunnel.

La clé manuelle est définie grâce à une fenêtre de saisie.

Dans l'onglet « Extrémités du trafic », vous précisez quelles machines vont utiliser ce tunnel et éventuellement pour quel type de connexions.

Vous sélectionnez les machines ou réseaux locaux en cliquant sur la machine de gauche et les machines ou réseaux distants en cliquant sur la machine de droite.

Dans un tunnel statique il est interdit d'avoir « Any » en correspondant.

Section B
PPTP

Principe

Le protocole PPTP permet de se connecter à distance sur le réseau local de manière sécurisée. Le poste client dispose d'un client PPTP (disponible sous Windows en standard ou MAC OSX) qui vient se connecter au firewall et identifier l'utilisateur.

L'utilisateur s'identifie par login/mot de passe. Ces profils sont stockés sur le firewall, dans la base LDAP contenant les fiches des utilisateurs internes.

Attention, l'utilisation d'IPSEC est préférable par rapport au PPTP car le niveau de sécurité est plus élevé.

© Copyright NETASQ 2006

Mise en place

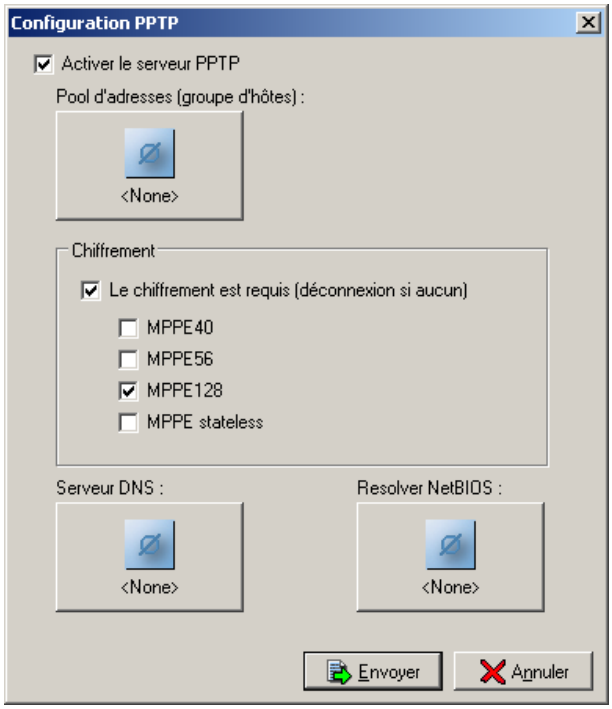
La mise en place est très simple et rapide. Elle se déroule en trois étapes :

Etape 1

Création d'un pool d'adresses IP privées. L'IPS-Firewall affecte au client qui vient se connecter en PPTP une adresse IP disponible dans le pool. Il faut créer un groupe de machines contenant les adresses réservées (Voir la « Configuration des groupes de machines »).

Etape 2

Activation / Configuration du serveur PPTP sur l'IPS-Firewall. Cela est réalisé dans le menu Configuration >VPN > PPTP.



Ce menu permet la configuration des paramètres suivants :

- ► Le pool d'adresses,
- ► Les paramètres de chiffrement,
- ► Les Serveurs DNS et Resolver Netbios.

Pool d'adresses

Le pool d'adresses est un groupe de machines contenant les adresses IP réservées pour la connexion en PPTP (cf étape 1).

Paramètres de chiffrement

Les paramètres de chiffrement possibles sont :

Le chiffrement est requis	Autorise la connexion uniquement si le client chiffre les données.

© Copyright NETASQ 2006

MPPE 40	Autorise l'utilisation du protocole de chiffrement MPPE 40 bits.
MPPE 56	Autorise l'utilisation du protocole de chiffrement MPPE 56 bits.
MPPE 128	Autorise l'utilisation du protocole de chiffrement MPPE 128 bits.
MPPE Stateless	Permet de supprimer la conservation d'état du tunnel. Cela accélère un peu le chiffrement mais devient plus lent à reprendre en cas de perte de paquets.

Les serveurs DNS et Resolver NetBios

Le champ Serveur DNS permet d'envoyer l'adresse IP du serveur DNS au client.

Le champ « Resolver NetBIOS » permet d'envoyer au client l'adresse IP du serveur WINS du site.

Etape 3

Création des profils utilisateurs. La connexion en PPTP est authentifiée par login/mot de passe. Vous pouvez définir les mots de passe des utilisateurs PPTP dans les fiches utilisateur (voir section « Configuration des objets > Utilisateurs »).

Section C

VPN SSL

© Copyright NETASQ 2006

L'utilisation de la technologie IPSEC nécessite l'intervention d'un administrateur sur les postes client par l'installation d'un logiciel de gestion de tunnels VPN. Cela est contraignant lorsque le nombre des postes client à équiper (installation, configuration et maintenance) est important, difficile lorsqu'on cherche à se procurer un tel client pour des périphériques tels que des PDA et coûteux car il nécessite l'achat de licences pour chaque station concernée.

Grâce à la technologie VPN SSL NETASQ et à un simple navigateur WEB, l'utilisateur accède au portail d'authentification NETASQ qui lui permet de justifier son identité avant d'atteindre les ressources autorisées par l'administrateur. Les communications sont alors chiffrées en SSL, la confidentialité est assurée.

La configuration de cette fonctionnalité est disponible grâce au menu « VPN > VPN SSL » de l'arborescence de l'interface graphique.

Utilisation du VPN SSL avec l'IPS-Firewall NETASQ

Cette fonctionnalité peut vous permettre d'accéder aux ressources protégées (par l'IPS-Firewall) de votre entreprise et cela sans installation d'un logiciel client sur le poste d'utilisation. Le cas d'utilisation le plus évident est celui d'un utilisateur nomade qui voudrait pouvoir récupérer ses mails alors qu'il est en déplacement. Cela est déjà possible grâce au VPN IPSEC mais nécessite l'installation d'un logiciel client qui pénalise l'utilisateur nomade. Grâce à la technologie VPN SSL, l'utilisateur nomade va peut désormais récupérer ses mails (ou visiter le site intranet de l'entreprise, accéder à un serveur privé, etc) de manière sécurisée (les flux sont chiffrés) tout en ne nécessitant pas d'installation de logiciel client. L'utilisateur peut donc tout à fait se connecter depuis un cybercafé, un ordinateur qui ne lui appartient pas, etc.

Fonctionnement

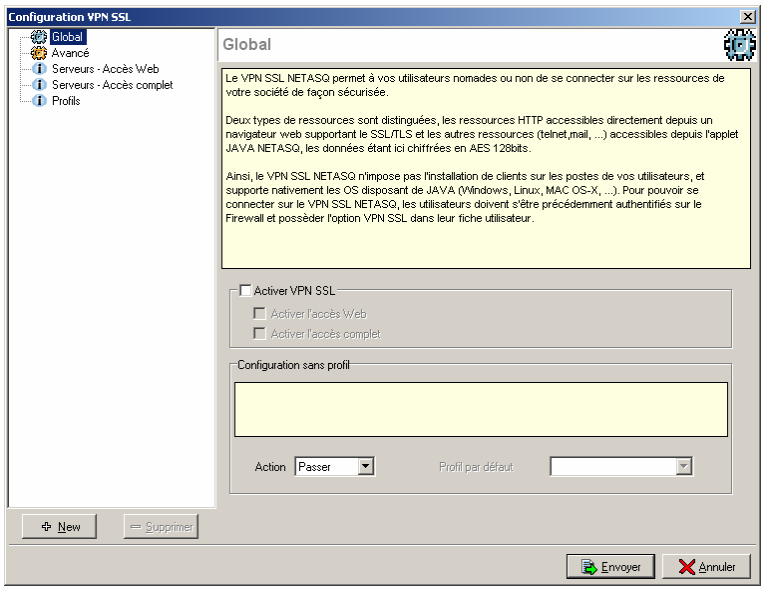
La technologie VPN SSL est divisée en deux fonctionnalités suivant le type d'accès que vous désirez réaliser : un accès à des ressources de type WEB (Intranet, Internet, etc) ou d'autres accès (serveur mail, serveurs d'applications privées).

L'écran de configuration du VPN SSL se décompose en deux parties :

- ► A gauche un arbre présentant les diverses fonctionnalités du menu VPN SSL,
- ► A droite les options configurables.

© Copyright NETASQ 2006

Global


Configuration VPN SSL
Global
Avancé
Serveurs - Accès Web
Serveurs - Accès complet
Profils
Global
Le VPN SSL NETASQ permet à vos utilisateurs nomades ou non de se connecter sur les ressources de votre société de façon sécurisée.
Deux types de ressources sont distinguées, les ressources HTTP accessibles directement depuis un navigateur web supportant le SSL/TLS et les autres ressources (telnet,mail, ...) accessibles depuis l'applet JAVA NETASQ, les données étant ici chiffrées en AES 128bits.
Ainsi, le VPN SSL NETASQ n'impose pas l'installation de clients sur les postes de vos utilisateurs, et supporte nativement les OS disposant de JAVA (Windows, Linux, MAC OS-X, ...). Pour pouvoir se connecter sur le VPN SSL NETASQ, les utilisateurs doivent s'être précédemment authentifiés sur le Firewall et possèder l'option VPN SSL dans leur fiche utilisateur.
Activer VPN SSL
Activer l'accès Web
Activer l'accès complet
Configuration sans profil
Action
Passer
Profil par défaut
New
Supprimer
Envoyer
Annuler

Activation du VPN SSL

Activer le VPN SSL	Sélectionnez cette option pour activer le module de VPN SSL.
Accès WEB	Utilisation du module de VPN SSL pour l'accès aux ressources de type WEB.
Autres Accès	Utilisation du module de VPN SSL pour l'accès aux ressources de type autre que le WEB.

La différence entre les deux technologies réside dans l'utilisation d'une applet JAVA pour l'accès aux ressources autre que le WEB. Cette applet JAVA insérée dans les pages du portail WEB NETASQ permet la redirection des flux vers les serveurs autorisés.

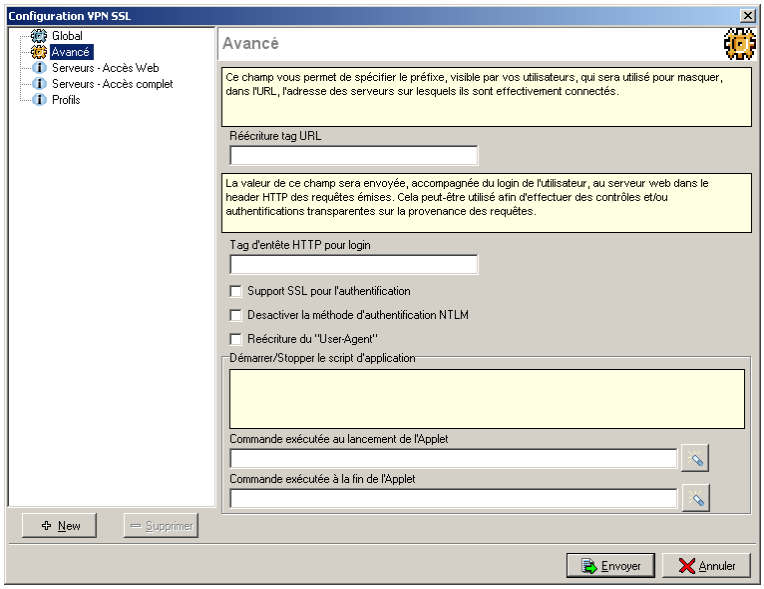
Configuration sans profil

Les options de la « configuration sans profil » permettent de déterminer les différents accès aux fonctionnalités de VPN SSL des IPS-Firewalls si l'utilisateur ne possède pas de profil spécifique défini dans sa fiche utilisateur (voir configuration des objets). Ces accès sont expliqués dans le tableau suivant :

Passer	Si l'action de la « configuration sans profil » est « Passer » alors tous les serveurs configurés par l'administrateur seront vu par un utilisateur sans profil spécifique.
Bloquer	Si l'action de la « configuration sans profil » est « Bloquer » alors aucun serveur configuré par l'adminstrateur ne sera vu par un utilisateur sans profil spécifique.
Défaut	Si l'action de la « configuration sans profil » est « Défaut » alors les serveurs configurés par l'administrateur et faisant partie du « profil par défaut » seront vu par un utilisateur sans profil spécifique.

© Copyright NETASQ 2006

Avancé


Configuration VPN SSL
Global
Avancé
Serveurs - Accès Web
Serveurs - Accès complet
Profils
Avancé
Ce champ vous permet de spécifier le préfixe, visible par vos utilisateurs, qui sera utilisé pour masquer, dans l'URL, l'adresse des serveurs sur lesquels ils sont effectivement connectés.
Réécriture tag URL
La valeur de ce champ sera envoyée, accompagnée du login de l'utilisateur, au serveur web dans le header HTTP des requêtes émises. Cela peut-être utilisé afin d'effectuer des contrôles et/ou authentifications transparentes sur la provenance des requêtes.
Tag d'entête HTTP pour login
Support SSL pour l'authentification
Desactiver la méthode d'authentification NTLM
Reécriture du "User-Agent"
Démarrer/Stopper le script d'application
Commande exécutée au lancement de l'Applet
Commande exécutée à la fin de l'Applet
New
Supprimer
Envoyer
Annuler

Préfixe de réécriture des URL

La technologie VPN SSL NETASQ permet de masquer l'adresse réelle des serveurs vers lesquels les utilisateurs sont redirigés en réécrivant l'ensemble des URL contenues dans les pages HTTP rencontrées. Ces URL sont remplacées par un préfixe suivi de 4 chiffres. Ce champ permet de définir le préfixe qui sera utilisé.

Marquage des entêtes HTTP pour le login

Dans le cas où le serveur vers lequel les flux HTTP sont redirigés demande une authentification, il est possible de spécifier un login dans l'entête du paquet HTTP. Ce login pourrait servir par exemple à indiquer que ces flux arrivant au serveur proviennent de l'IPS-Firewall et peuvent être accepté par le serveur sans authentification.

Support SSL pour l'authentification

Si l'option « Support SSL pour l'authentification » est cochée, chaque requête transitant par le module de VPN SSL des IPS-Firewalls NETASQ nécessite une authentification par certificat de l'utilisateur emetteur de la requête.

Désactiver la méthode d'authentification NTLM

Certains serveurs WEB peuvent demander une authentification préalable au transfert de flux entre le serveur et l'utilisateur. Ne supportant pas cette méthode d'authentification pour les trafics traversant l'IPS-Firewall, celle-ci peut être désactivée. Ainsi l'utilisateur ne peut jamais choisir cette méthode pour son authentification sur le serveur WEB distant.

Réécriture du « User-Agent »

Le champ « User-Agent » de l'entête d'une requête HTTP contient l'identifiant de navigateur WEB utilisé par l'utilisateur. Pour Internet Explorer par exemple : Mozilla/4.0 (compatible; MSIE 6.0 ...). La réécriture du « User-Agent » permet donc de modifier la requête HTTP de telle façon que l'on pense qu'elle provient d'un autre type de navigateur qu'en réalité.

Cette option est notamment utile dans une utilisation dégradée de « Outlook Web Access » (OWA). En effet, « Outlook Web Access » (OWA) en mode premium, mode très évolué de « Outlook Web Access » fait appel au Webdav, une extension du protocole HTTP. Ces extensions n'étant pas supportées par tous les équipements réseau (le mode premium de OWA est supporté par le module VPN SSL des IPS-Firewalls NETASQ), le transit de ces trafics pourrait poser des problèmes de compatibilité en particulier sur Internet. Plutôt que de devoir dégrader l'utilisation de OWA pour tous

les utilisateurs (interne et externe), l'option « Réécriture du « User-Agent » permet une utilisation « premium » de OWA en interne (compatibilité avec le mode premium facile à obtenir) et une utilisation « dégradée » en passant par le VPN SSL (utilisé par les utilisateurs normades, via Internet). En effet les « vieux » navigateurs WEB ne supportent pas ces extensions, OWA fonctionne donc automatiquement en mode dégradé lorsqu'il rencontre le « User-Agent » de ces navigateurs.

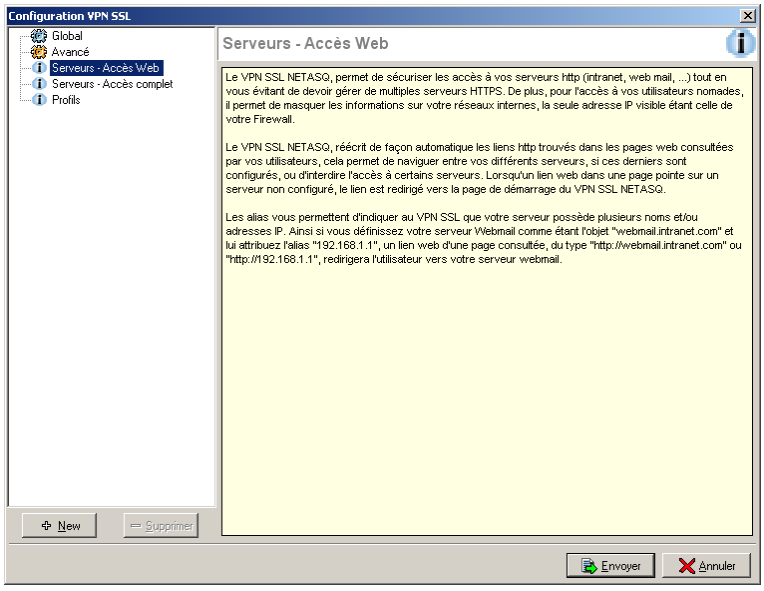
Commande exécutée au lancement de l'applet

Exécuté au lancement de l'applet, cette commande permet à l'administrateur de définir des actions préalables à l'affichage de l'applet. Par exemple, cette commande pourrait lancer un script présent sur un serveur et qui modifierait les paramètres du compte de messagerie de l'utilisateur de telle façon que lorsque l'applet est lancée, les flux SMTP ou POP soit automatiquement redirigé, sans intervention de l'utilisateur.

Commande exécutée à la fin de l'applet

Exécuté à la fermeture de l'applet, cette commande permet à l'administrateur de définir des actions préalables à la fermeture de l'applet. Par exemple, cette commande pourrait lancer un script présent sur un serveur et qui modifierait les paramètres du compte de messagerie de l'utilisateur de telle façon que lorsque l'applet est fermée, les flux SMTP ou POP ne sont plus automatiquement redirigé et encore une fois sans intervention de l'utilisateur.

Accès WEB


Configuration VPN SSL
Global
Avancé
Serveurs - Accès Web
Serveurs - Accès complet
Profils
Serveurs - Accès Web
Le VPN SSL NETASQ, permet de sécuriser les accès à vos serveurs http (intranet, web mail, ...) tout en vous évitant de devoir gérer de multiples serveurs HTTPS. De plus, pour l'accès à vos utilisateurs nomades, il permet de masquer les informations sur votre réseaux internes, la seule adresse IP visible étant celle de votre Firewall.
Le VPN SSL NETASQ, réécrit de façon automatique les liens http trouvés dans les pages web consultées par vos utilisateurs, cela permet de naviguer entre vos différents serveurs, si ces derniers sont configurés, ou d'interdire l'accès à certains serveurs. Lorsqu'un lien web dans une page pointe sur un serveur non configuré, le lien est redirigé vers la page de démarrage du VPN SSL NETASQ.
Les alias vous permettent d'indiquer au VPN SSL que votre serveur possède plusieurs noms et/ou adresses IP. Ainsi si vous définissez votre serveur Webmail comme étant l'objet "webmail.intranet.com" et lui attribuez l'alias "192.168.1.1", un lien web d'une page consultée, du type "http://webmail.intranet.com" ou "http://192.168.1.1", redirigera l'utilisateur vers votre serveur webmail.
New
Supprimer
Envoyer
Annuler

Cette section rassemble les serveurs configurés pour les accès aux ressources de type WEB.

Ajouter un serveur d'accès WEB

Pour ajouter un serveur d'accès WEB, suivez la procédure suivante :

1. Cliquez sur le bouton « Nouveau » situé en bas de la fenêtre de configuration du VPN SSL, puis sélectionnez « Serveur HTTP » ;

2. Indiquez un nom pour ce serveur ;

3. La configuration de ce serveur apparaît alors, les explications des différents paramètres sont données dans le tableau ci-dessous.

Lien sur le portail WEB	Le lien défini apparaît sur le portail WEB NETASQ. Lorsque l'utilisateur clique sur ce lien, il est redirigé vers le serveur correspondant.
Serveur	Ce champ permet de spécifier l'objet correspondant au serveur auquel l'utilisateur pourra accéder. **Veillez à utiliser un objet dont le nom est identique au nom FQDN du serveur auquel il fait référence. Si cela n'est pas le cas (nom de l'objet : webmail, nom FQDN : www.webmail.com par exemple), il est possible que les requêtes de l'IPS-Firewall auprès de ce serveur soient refusées.**
Port	Champ permettant de spécifier le port du serveur auquel l'utilisateur veut accéder. Par défaut le port défini est 80 : HTTP.
URL	Cette URL permet d'arriver directement sur la page spécifiée.
Liste d'alias du serveur	Les alias permettent d'indiquer au module VPN SSL que le serveur possède plusieurs noms et/ou adresses IP. Si un serveur de mails est défini comme l'objet « webmail.intranet.com » auquel on assigne l'alias « 192.168.1.1 », lorsque le lien visité sera « http://webmail.intranet.com » ou « http://192.168.1.1 » l'utilisateur sera redirigé vers le serveur de mails.
Liste blanche	Seuls les liens réécrits par le module VPN SSL sont accessibles au travers du VPN SSL. S'il existe sur un site autorisé un lien vers un site WEB extérieur (dont le serveur n'est pas défini dans la configuration VPN SSL), celui-ci sera inacessible par le VPN SSL. Lorsque la liste blanche est activée, elle permet l'accès à des URLs qui ne seraient pas réécrites. Attention lorsqu'un lien de cette liste blanche est cliqué par un utilisateur, celui-ci n'est plus protégé par le module de VPN SSL NETASQ.
Ne pas afficher ce serveur sur le portail	Tous les serveurs configurés dans la configuration du VPN SSL sont par défaut indiqués sur le portail d'authentification NETASQ. Toutefois il pourrait être nécessaire qu'un de ces serveurs ne soit accessible que par l'intermédiaire d'un autre serveur, alors, dans ce cas, il faudrait cocher l'option « Ne pas afficher ce serveur sur le portail ». En effet lorsque cette option est cochée dans la configuration d'un serveur, ce serveur est accessible par le VPN SSL mais n'est pas présent dans la liste d'accès direct. Il faut un lien sur un serveur vers ce serveur pour y accéder.

Retirer un serveur

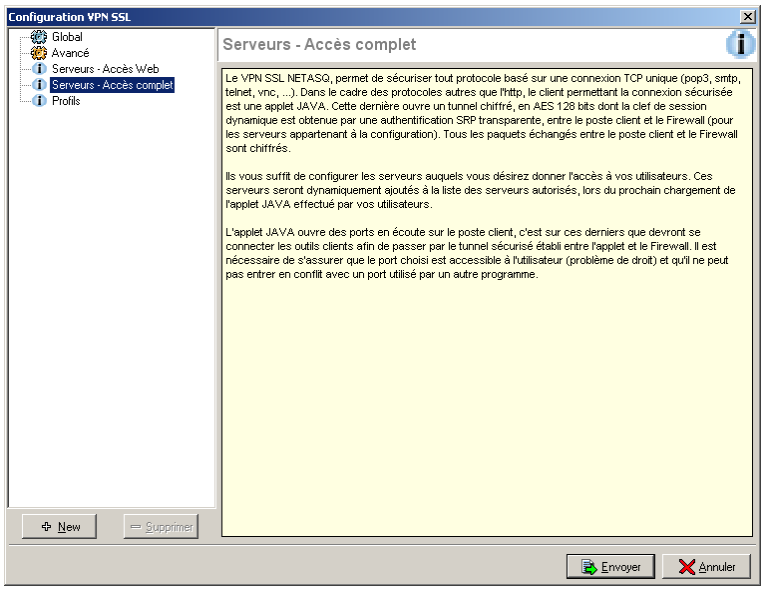
Pour supprimer un serveur, suivez la procédure suivante :

1. Sélectionnez le serveur à supprimer ;
2. Cliquez sur le bouton « Supprimer ».

Ajouter un serveur HTTP -OWA

Le module VPN SSL des IPS-Firewalls NETASQ supporte les serveurs OWA (« Outlook Web Access »), il est donc possible d'ajouter dans la liste des serveurs d'accès WEB, un serveur HTTP avec certaines options spécifiquement préremplies pour une parfaite compatibilité avec OWA. Pour cela sélectionnez l'option « Nouveau\Serveur HTTP – OWA » plutôt que « Nouveau\Serveur HTTP ». Les autres options non remplies doivent être configurées de la manière que pour un serveur d'accès WEB « normal ».

Accès complet


Configuration VPN SSL
Global
Avancé
Serveurs - Accès Web
Serveurs - Accès complet
Profils
Serveurs - Accès complet
Le VPN SSL NETASQ, permet de sécuriser tout protocole basé sur une connexion TCP unique (pop3, smtp, telnet, vnc, ...). Dans le cadre des protocoles autres que l'http, le client permettant la connexion sécurisée est une applet JAVA. Cette dernière ouvre un tunnel chiffré, en AES 128 bits dont la clef de session dynamique est obtenue par une authentification SRP transparente, entre le poste client et le Firewall (pour les serveurs appartenant à la configuration). Tous les paquets échangés entre le poste client et le Firewall sont chiffrés.
Ils vous suffit de configurer les serveurs auquels vous désirez donner l'accès à vos utilisateurs. Ces serveurs seront dynamiquement ajoutés à la liste des serveurs autorisés, lors du prochain chargement de l'applet JAVA effectué par vos utilisateurs.
L'applet JAVA ouvre des ports en écoute sur le poste client, c'est sur ces derniers que devront se connecter les outils clients afin de passer par le tunnel sécurisé établi entre l'applet et le Firewall. Il est nécessaire de s'assurer que le port choisi est accessible à l'utilisateur (problème de droit) et qu'il ne peut pas entrer en conflit avec un port utilisé par un autre programme.
New
Supprimer
Envoyer
Annuler

Cette section rassemble les serveurs configurés pour les accès aux ressources autres que le type WEB.

Ajouter un serveur d'accès aux ressources autres que le type WEB

Pour ajouter un serveur d'accès aux ressources autres que le type WEB, suivez la procédure suivante :

1. Cliquez sur le bouton « Nouveau » situé en bas de la fenêtre de configuration du VPN SSL, puis sélectionnez « Autre Serveur » ;

2. Indiquez un nom pour ce serveur ;

3. La configuration de ce serveur apparaît alors, les explications des différents paramètres sont données dans le tableau ci-dessous.

Port d'écoute	Ce port situé sur la station distante est utilisé par l'applet JAVA pour la redirection des flux chiffrés à destination de l'IPS-Firewall NETASQ. Notez que l'utilisateur doit posséder certains droits sur ce port (pour l'ouverture par exemple), veillez donc à modifier les droits locaux d'administration de la machine en conséquence. De plus, le port spécifié doit être libre d'utilisation sur toutes les machines désirant se connecter au serveur associé via le portail.
Serveur	Ce champ permet de spécifier l'objet correspondant au serveur auquel l'utilisateur pourra accéder.
Port	Ce champ permet de spécifier le port sur le serveur auquel l'utilisateur pourra accéder.
Commande exécutée au lancement de l'applet	Exécuté au lancement de l'applet, cette commande permet à l'administrateur de définir des actions préalables à l'affichage du serveur. Par exemple, cette commande pourrait lancer un script présent sur un serveur et qui vérifierait l'activité de l'antivirus présent sur la machine de l'utilisateur avant de lui donner accès au serveur.

Retirer un serveur

Pour supprimer un serveur, suivez la procédure suivante :

1. Sélectionnez le serveur à supprimer ;

2. Cliquez sur le bouton « Supprimer ».

Lorsqu'un serveur est retiré de la liste des serveurs VPN SSL configurés, il est automatiquement retiré des profils auxquels il faisait partie.

Profils

Principe de fonctionnement

Par défaut tous les serveurs configurés dans le module VPN SSL sont affichés sur le portail d'authentification. Ainsi tous les utilisateurs ayant droit aux fonctionnalités de VPN SSL offertes par l'IPS-Firewall ont accès à tous les serveurs configurés par l'administrateur. La notion de profil permet de déterminer quels utilisateurs auront accès à quels serveurs configurés dans le VPN SSL.

Configurer un profil

Ajouter un profil

Pour ajouter un profil dans la liste des profils VPN SSL disponibles, reportez-vous à la procédure suivante :

1. Cliquez sur le bouton « Nouveau » situé en bas de la fenêtre de configuration du VPN SSL, puis spécifiez le nom du profil en accord avec les recommandations indiquées par la fenêtre de définition du nom du profil ;

2. Sélectionnez dans les listes de serveurs d'accès WEB et d'accès complet, les serveurs qui seront accessibles aux utilisateurs appartenant à ce profil ;

3. Cliquez sur « Envoyer » pour activer la configuration

Il est impossible de créer un profil s'il n'existe pas au minimum 1 serveur VPN SSL configuré.

Supprimer un profil

Pour supprimer un profil, reportez-vous à la procédure suivante :

1. Sélectionnez le profil à supprimer ;

2. Cliquez sur le bouton « Supprimer ».

Utiliser un profil

Un profil peut être utilisé de 2 manières différentes. Soit il est utilisé comme profil par défaut dans la configuration du VPN SSL, soit il est assigné à un ou plusieurs utilisateurs comme profil spécifique de ces utilisateurs.

Utiliser un profil comme profil par défaut

Pour utiliser un profil comme profil par défaut de la configuration VPN SSL (tous les utilisateurs n'utilisant pas de profil spécifique seront affectés par ce profil par défaut), reportez-vous à la procédure suivante :

1. Définissez le profil qui sera utilisé comme profil par défaut (nom du profil et serveurs associés) dans le menu de configuration des profils ;

2. Dans le menu « Global » de la configuration VPN SSL, sélectionnez l'action « Défaut » de la configuration sans profil ;

3. Indiquez le profil, que vous avez préalablement défini, dans l'option « Profil par défaut », puis cliquez sur « envoyez » pour appliquer les modifications.

Utiliser un profil comme profil spéficique d'un ou pluseurs utilisateurs.

Pour utiliser un profil comme profil spécifique d'un ou plusieurs utilisateurs (quelle que soit la liste des serveurs définis par le profil par défaut, ces utilisateurs posséderont une liste de serveurs spécifiques), reportez-vous à la procédure suivante :

1. Définissez le profil qui sera utilisé comme profil par défaut (nom du profil et serveurs associés) dans le menu de configuration des profils puis appliquez les modifications en cliquant sur « Envoyer » ;

2. Sélectionnez, dans la liste des utilisateurs du menu « Objets » de l'arborescence des menus du Firewall Manager, l'utilisateur auquel vous désirez asscocié le profil préalablement défini ;

3. Sélectionnez l'onglet « Accès » de sa fiche utilisateur et cochez l'option « Par VPN SSL » (si cela n'est pas déjà fait) ;

4. Cochez l'option « Utiliser un profil spécifique » et indiquez le profil que vous désirez associer à cet utilisateur, puis cliquez sur « envoyez » pour appliquer les modifications.

Services VPN SSL sur le portail WEB NETASQ

Lorsque l'authentification sur l'IPS-Firewall est activée (Voir « Configuration de l'authentification »), le portail WEB NETASQ permet aux utilisateurs d'accéder aux fonctionnalités du VPN SSL NETASQ.

Pour accédez aux fonctionnalités du VPN SSL, suivez la procédure suivante :

1. Ouvrir un navigateur WEB,

2. Indiquer dans la barre d'adresse, l'URL : https://Adresse_Firewall

3. La page d'authentification sur l'IPS-Firewall apparaît, l'utilisateur doit se connecter,

4. Si l'utilisateur possède des droits sur l'utilisation des fonctionnalités VPN (Voir « Droits de l'utilisateur ») le menu « Accès sécurisé » apparaît, il permet d'accéder aux fonctionnalités VPN SSL.

Accédez aux sites WEB de votre entreprise par un tunnel SSL

Ce menu présente les sites WEB configurés par l'administrateur et auxquels les utilisateurs peuvent accéder.

Le lien « Les autres accès sécurisés sont ici » permet d'accéder au menu des autres sites sécurisés configurés par l'administrateur

Accédez aux ressources de votre entreprise par un tunnel SSL

Ce menu présente les autres serveurs configurés par l'administrateur et auxquels les utilisateurs peuvent accéder.

Sur cette page aucun lien n'est disponible. Il est pourtant indispensable que cette fenêtre reste ouverte pendant toute la durée de la connexion (elle peut être minimisée). La fermeture de la fenêtre entraîne la coupure de la connexion.

Pour accéder aux ressources configurées par l'administrateur, il s'agit d'indiquer au logiciel client, un client de messagerie par exemple, que le serveur auquel il doit se connecter pour récupérer les mails n'est plus le serveur Mail habituel mais il faut lui indiquer une adresse du type « 127.0.0.1:Port_Ecoute » où « Port_Ecoute » est le port spécifié dans la configuration du serveur.

Le port d'écoute pour chacun des serveurs configurés est rappelé dans la page du portail WEB NETASQ.

Chapitre VI

Configuration des proxies

© Copyright NETASQ 2006

Section A

Proxies HTTP, SMTP et POP3

© Copyright NETASQ 2006

Pour cette section, vous devez avoir franchi les étapes

► Installation, pré-configuration, intégration,
► Configuration des objets.

Pour cette section, vous devez connaître

► Les noms de domaines autorisés à sortir de votre réseau en SMTP et POP3,
► La politique de filtrage d'Emails que vous voulez mettre en place,
► Les adresses des différents proxies.

Utilité de la section

Cette section vous permet d'activer les proxies HTTP, SMTP, de rediriger les flux HTTP vers des serveurs proxies externes et de filtrer les flux SMTP et POP3.

Accéder à cette section

Accédez à la boîte de dialogue par le menu « Proxies ».

Vous devez être connecté avec les privilèges de modification pour pouvoir effectuer ces modifications.

Avant d'effectuer toute modification importante sur votre Firewall NETASQ, nous vous conseillons d'effectuer une sauvegarde. Ainsi, en cas de mauvaise manipulation vous pourrez vous retrouver dans l'état précédent. Pour plus d'informations sur les sauvegardes, veuillez vous référer au chapitre « Sauvegarde et restauration ».

Introduction à cette section

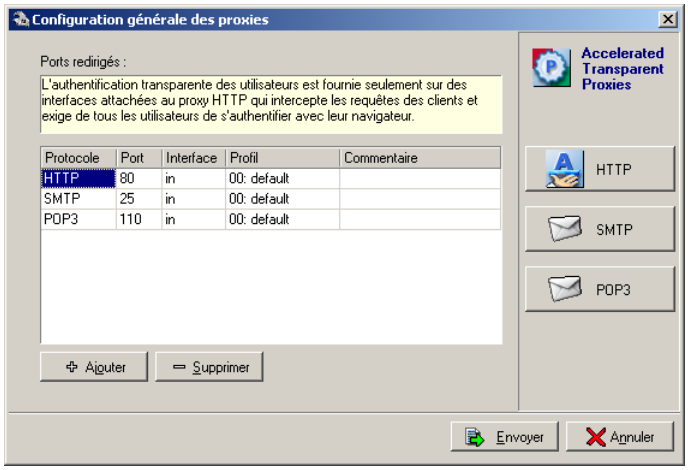
Les tables de filtrage URL sont stockées sur le Firewall NETASQ dans des slots (fichiers de configuration numérotés de 01 à 10).

Chaque slot peut être programmé à une heure précise de la semaine, en écrasant la configuration du slot précédemment activée. (Voir « Programmation des slots »)

© Copyright NETASQ 2006

Vous avez la possibilité de choisir sur quels ports et interfaces les proxies vont agir. Lorsqu'une connexion provient de l'interface indiquée et demande le service configuré dans cette partie, le proxy intercepte et gère la connexion.

On accède à cette configuration dans le menu « Proxies > Général ».



La redirection des flux vers les proxies nécessite la définition des paramètres suivants :

Protocole	Protocole géré par le proxy.
Port	Port sur lequel le proxy doit écouter.
Interface	Interface sur laquelle le proxy écoute.
Profil	Permet d'associer un profil Proxy à l'analyse réalisée par les proxies. Pour permettre des configurations différentes suivant les interfaces par exemple.
Commentaire	Commentaire associé à cette ligne.

On ajoute un port ou interface à filtrer avec les boutons ajouter/supprimer. Par défaut, le filtrage URL (proxy HTTP) s'applique sur le port 80 pour les machines du réseau interne uniquement, le filtrage SMTP s'applique sur le port 25 pour les machines du réseau interne et le filtrage POP3 s'applique sur le port 110 pour les machines du réseau interne aussi.

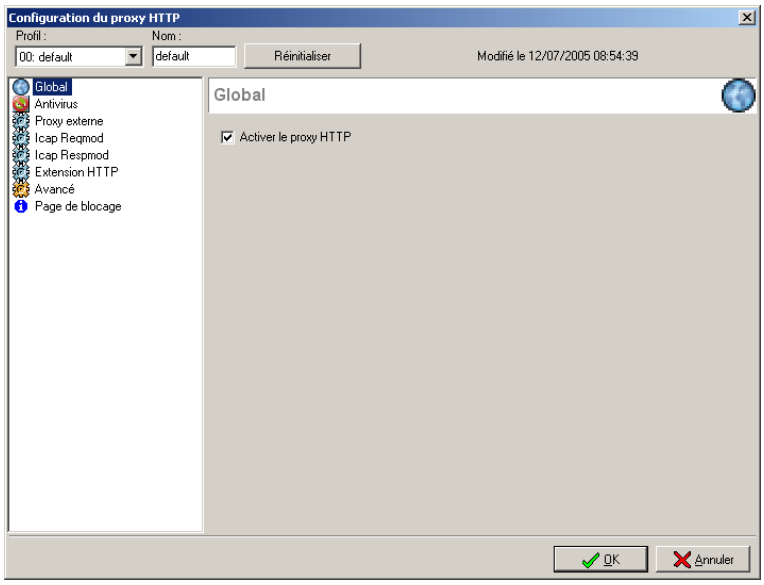
Le filtrage URL entre en application lorsqu'un fichier de règles est activé (voir section filtrage URL).

Le filtrage URL est prioritaire sur le filtrage par protocole. Les règles de filtrage correspondant aux ports filtrés par le module de filtrage URL ne sont pas prises en compte. Vous appliquez donc les règles d'accès Internet uniquement au niveau du filtrage URL. Si vous activez un slot de filtrage d'URLs, le proxy sera automatiquement activé.

Remarque : l'authentification transparente (la page d'authentification est automatiquement proposée à l'utilisateur lorsqu'il désire se connecter à Internet) est fournie seulement aux interfaces liées au proxy HTTP qui intercepte les requêtes clientes. Le filtrage URL ne s'applique pas sur les requêtes HTTPS.

© Copyright NETASQ 2006

Pour utiliser le proxy HTTP, celui-ci doit être activé. L'activation du proxy est réalisée au niveau de la section « Proxy HTTP » du menu « Proxies » de l'arborescence.



Ce menu est divisé en deux parties :

- ► A gauche un arbre présentant les diverses fonctionnalités du menu Proxy HTTP,
- ► A droite les options configurables.

Il est désormais possible de créer quatre profils pour le Proxy afin d'adapter l'analyse du proxy en fonction du sens du trafic. Cela va permettre de désactiver certaines fonctionnalités sur les trafics autorisés en sortie mais pas en entrée.

La barre d'action située en haut de l'écran vous indique quel profil du proxy HTTP est actuellement affiché. De plus vous pouvez spécifier un nom pour chacun des quatre profils.

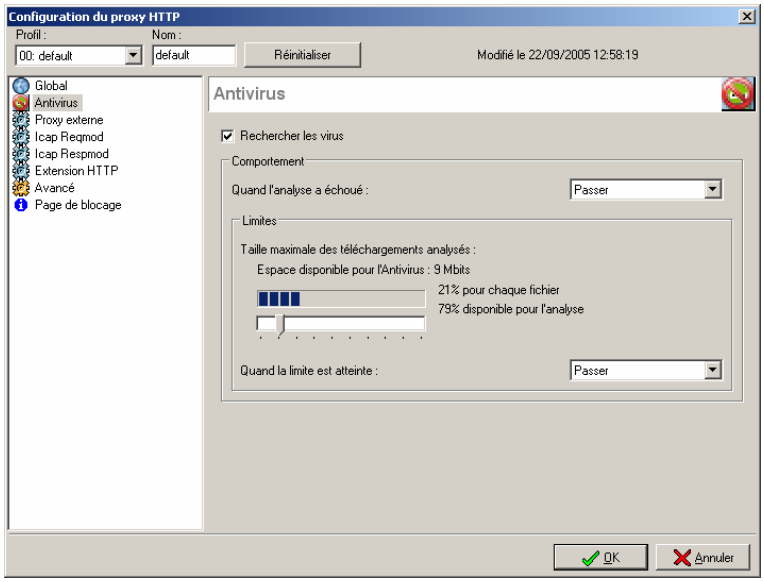
Le bouton « Réinitialiser » vous permet de redéfinir les paramètres des profils du proxy HTTP dans leur configuration d'origine.

La date située à côté du bouton « Réinitialiser » indique la date de la dernière modification de la configuration.

Cochez l'option « Activer le proxy HTTP » dans le menu « Global » pour activer le proxy HTTP et effectuer les analyses spécifiées dans les menus suivants.

© Copyright NETASQ 2006

Antivirus



L'activation du proxy HTTP permet notamment l'activation de la recherche des virus dans les trafics HTTP (uniquement sur les requêtes GET). Pour activer la recherche des virus reportez-vous à la procédure suivante :

1. Activer le proxy HTTP en cochant l'option « Activer le proxy HTTP » dans le menu « Global » ;

2. Activer la recherche des virus en cochant l'option « Recherche des virus » dans le menu « Antivirus » ;

3. Cliquer sur OK pour valider les modifications.

Comportement

La section « Comportement » décrit le comportement de l'antivirus face à certains événements.

L'option « Lorsque l'analyse échoue » définit le comportement de l'antivirus si l'analyse du fichier qu'il est en train de scanner échoue (il ne réussit pas à analyser le fichier parce qu'il est verrouillé par exemple).

Si « Bloquer » est spécifié, le fichier en cours d'analyse n'est pas transmis.
Si « Passer » est spécifié, le fichier en cours d'analyse est transmis.

Limitation

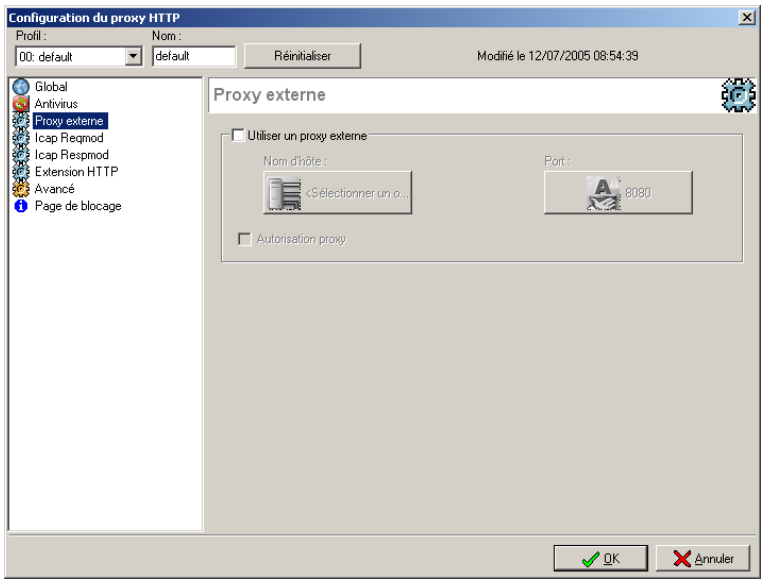
La « Taille limite des données analysées » est fonction des capacités matérielle chaque modèle d'IPS-Firewall mais elle peut être adaptée selon les besoins de l'entreprise. Pour cela, déplacez la règlette.

Attention lorsque vous définissez une taille limite de données analysées manuellement, veillez à conserver un ensemble de valeurs cohérentes. En effet, l'espace mémoire total, représenté par la réglette correspond à l'ensemble des ressources réservées pour le service Antivirus. Si vous définissez que la taille limite des données analysées sur HTTP est de 100% de la taille total, aucun autre fichier ne pourra être analysé en même temps.

L'option « Lorsque la limite est dépassé » définit le comportement de l'antivirus si la taille du fichier d'analyse qu'il est en train de scanner dépasse la limite autorisée.

Si « Bloquer » est spécifié, le fichier en cours d'analyse n'est pas transmis.
Si « Passer » est spécifié, le fichier en cours d'analyse est transmis.

Proxy externe



Le proxy HTTP sert pour le filtrage d'URLs (voir section "Configuration du filtrage d'URL") mais il permet aussi de rediriger les requêtes HTTP provenant des utilisateurs du réseau interne vers des proxies externes.

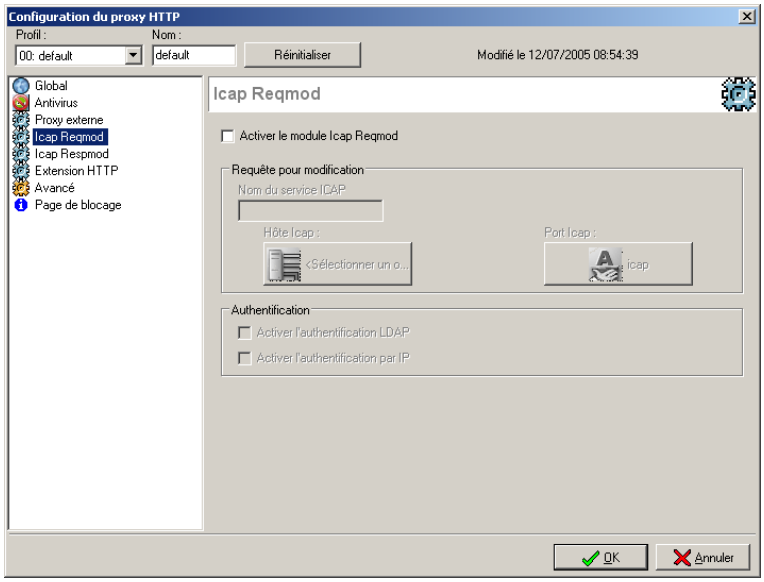
Pour activer cette redirection, cochez la case correspondante puis précisez l'adresse IP du serveur ainsi que le port sur lequel il reçoit les requêtes. Si l'administrateur spécifie un groupe de serveurs dans l'option « Nom d'hôte », l'IPS-Firewall effectuera un partage de charge entre les différentes proxies externes du groupe en fonction de la machine source (une machine source donnée utilisera toujours le même proxy externe).

Autorisation proxy

Si le proxy HTTP externe nécessite une authentification des utilisateurs, l'administrateur peut cocher l'option « Autorisation proxy » présente dans le menu « Proxy externe » pour envoyer au proxy externe les informations concernant l'utilisateur recueuillies par le module d'authentification de l'IPS-Firewall.

© Copyright NETASQ 2006

Configuration ICAP



ICAP ou Internet Content Application Protocol est un protocole d'adaptation de contenu. Il assure une interopérabilité avec des solutions d'analyse et de traitement de contenu comme WebWasher et permet des services de filtrage d'URLs ou de filtrage de contenu. Il fonctionne selon deux modes : le Reqmod et le Respmod.

Le Reqmod (Request for Modification) fonctionne selon le principe suivant :

► Un client HTTP envoie une requête HTTP,
► Celle-ci traverse le firewall et est interceptée par le serveur ICAP,
► Le serveur ICAP renvoie une réponse au firewall qui la transmet au serveur WEB concerné.

Le Respmod fonctionne dans le sens inverse.

Le firewall NETASQ supporte les deux modes.

ICAP respmod et ICAP reqmod

Pour chacun des menus, trois informations sont nécessaires pour mettre en place les services ICAP :

► Le nom du service à mettre en place, cette information est différente suivant la solution utilisée,
► Le serveur ICAP,
► Ainsi que le port utilisé.

Il est impossible d'utiliser le respmod ICAP lorsque la recherche de virus sur HTTP est activée.

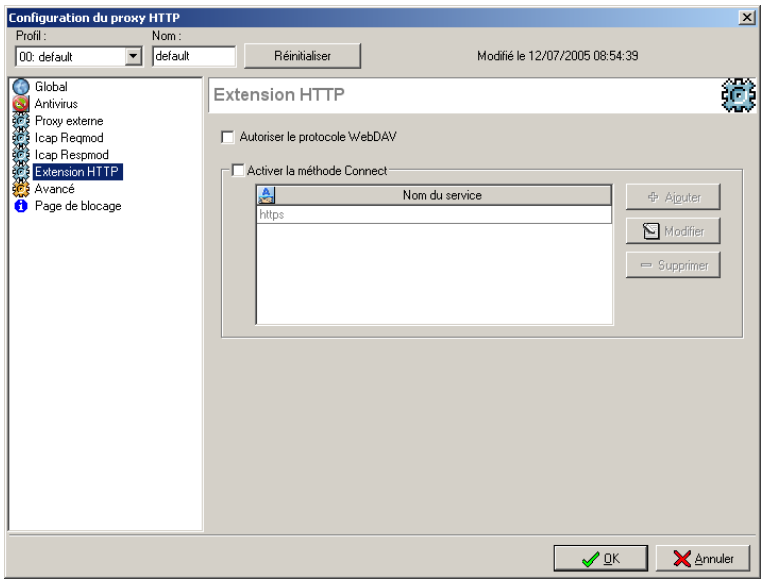
Authentification

On peut utiliser les informations disponibles sur le firewall pour réaliser des services ICAP. Par exemple, il est possible de définir dans un serveur ICAP que tel ou tel site n'est destiné qu'à telle ou telle personne. Dans ce cas, vous pouvez filtrer selon un identifiant LDAP ou une adresse IP.

L'option « Activer l'authentification LDAP » permet de se servir des informations relatives à la base LDAP (notamment l'identifiant d'un utilisateur authentifié).

L'option « Activer l'authentication par IP » permet de se servir des adresses IP des clients HTTP effectuant la requête à « adapter ».

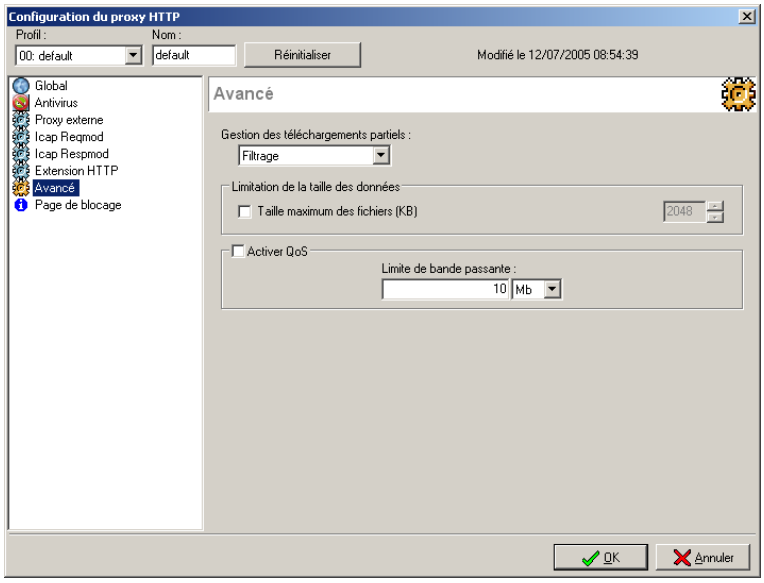
Onglet Extension HTTP



L'onglet « HTTP Extension » permet de configurer les paramètres suivants :

Autoriser le protocole WebDAV	WebDAV est un ensemble d'extensions au protocole HTTP concernant l'édition et la gestion collaborative de documents. Si cette option est cochée le protocole WebDav est autorisé au travers du firewall NETASQ.
Activer la méthode Connect	La méthode Connect permet de réaliser des tunnels sécurisés au travers de serveurs proxies. Le champ « Nom du service » sert à spécifier quels types de service peuvent utiliser une telle méthode. Si cette option est cochée la méthode « Connect » est autorisée au travers du firewall NETASQ.

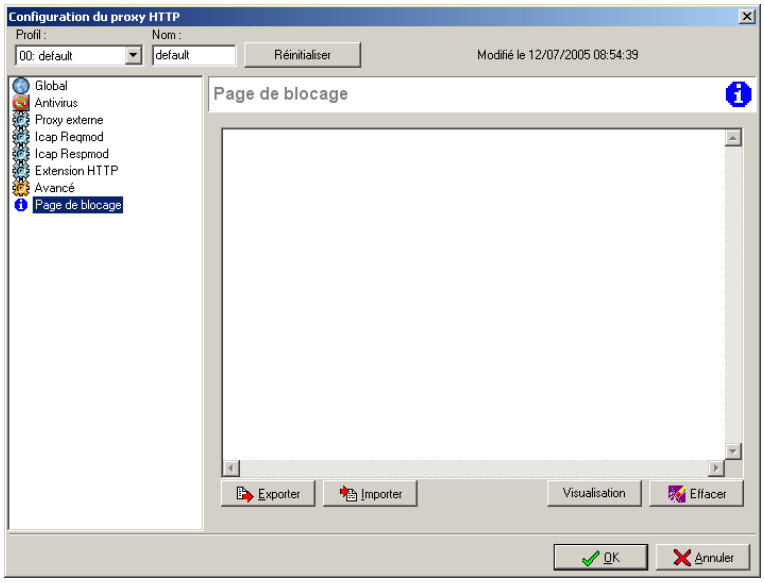
Onglet Avancé



L'onglet « Avancé » permet de configurer les paramètres suivants :

Gestion des téléchargements partiels	Par exemple lorsqu'on télécharge un fichier via FTP si le téléchargement ne s'effectue pas jusqu'au bout (erreur de connexion par exemple), il est possible de relancer le téléchargement à partir de là où a surgi l'erreur plutôt que de devoir tout retélécharger. Il s'agit dans ce cas d'un téléchargement partiel (le téléchargement ne correspond pas à un fichier complet). L'option « Gestion des téléchargements partiels » permet de définir le comportement du proxy HTTP de l'IPS-Firewall vis-à-vis de ce type de téléchargement. ► Bloquer : le téléchargement partiel est interdit ; ► Filtrage : le téléchargement partiel est autorisé et le trafic est filtré par l'antivirus ; ► Passer : le téléchargement partiel est autorisé mais il n'y a pas d'analyse antivirale effectuée.
Limite de données	Lorsque les fichiers téléchargés sur l'Internet, via HTTP sont trop imposants, ils peuvent dégrader la bande passante du lien Internet et cela pour une durée parfois très longue. Pour éviter cet écueil, cochez l'option « taille maximum des fichiers » et indiquez la taille maximum en Ko pouvant être téléchargé par le protocole HTTP.
Activer QoS	Régulation du trafic HTTP. Cette option vous permet de définir un débit maximum pour ce type de trafic. Un calcul de dérivée de la courbe du trafic permet de déterminer si des paquets doivent être supprimés silencieusement afin de ne pas dépasser le débit limite.

Page de blocage



La page de blocage est affichée lorsque la requête HTTP d'un utilisateur est rejetée par le proxy HTTP (URL non autorisée). Elle est accessible par le menu «Proxy > Proxy HTTP ».

Cette page s'affiche dans le navigateur de l'utilisateur à la place de la page WEB demandée.

Par défaut, une page NETASQ s'affiche, informant l'utilisateur que sa demande ne peut pas être acceptée, avec la règle de filtrage appliquée et l'URL demandée.

Vous pouvez remplacer cette page par défaut par votre propre page en entrant dans cette fenêtre le code HTML de la page à afficher.

Vous pouvez ajouter les informations suivantes dans cette page :

- $rule: règle de filtrage qui est appliquée,
- $host : le nom du destinataire HTTP (ex : www.google.com),
- $url : URL qui est bloquée (ex : /search?hl=fr&q=test&btng=rechercher&meta=).

Remarque

Pour créer vos propres messages de blocage, utilisez un éditeur HTML puis enregistrez le document au format HTML. Vous pouvez ensuite importer ce document avec le bouton « Importer ».

Toute page éditée dans la section « page de blocage » peut ensuite être enregistrée pour être importée sur un autre IPS-Firewall avec le bouton « Exporter ».

Vous avez la possibilité de visualiser le rendu de la page HTML éditée, en cliquant sur le bouton « Visualisation ». Cette action ouvre automatiquement le navigateur par défaut de votre machine.

Enfin si la page que vous avez configurée ne vous convient plus le bouton « Effacer » vous permet de la supprimer pour revenir à la page par défaut de NETASQ.

© Copyright NETASQ 2006

Introduction

Ces dernières années, la messagerie électronique est devenue un outil de communication largement utilisé par les entreprises et les administrations. La transmission rapide et performante des informations permet une amélioration notable de la compétitivité et une baisse des coûts.

Cependant, sans une gestion adéquate du trafic, l'usage de cet outil peut s'avérer désastreux pour la productivité.

Les courriers de masse non sollicités (tels que la publicité, les newsletters…) peuvent avoir des conséquences sur la disponibilité de votre bande passante. De plus, les messages infectés provenant de l'Internet sont autant de failles dans votre sécurité.

Ces écueils sont généralement imputables à une utilisation de l'outil de messagerie à des fins personnelles.

C'est le protocole SMTP : Simple Mail Transfer Protocol, protocole de communication TCP-IP, qui est utilisé pour les échanges de courrier électronique dans Internet.

Il s'agit d'un protocole fonctionnant en mode connecté, encapsulé dans une trame TCP/IP. Le courrier est remis directement au serveur de courrier du destinataire. Le protocole SMTP fonctionne grâce à des commandes textuelles envoyées au serveur SMTP (par défaut sur le port 25). Chacune des commandes envoyées par le client (validée par la chaîne de caractères ASCII CR/LF, équivalent à un appui sur la touche entrée) est suivie d'une réponse du serveur SMTP composée d'un numéro et d'un message descriptif.

Il est ainsi possible d'envoyer un courrier grâce à un simple telnet sur le port 25 du serveur SMTP.

Différentes utilisations possibles du proxy SMTP

Le proxy SMTP peut être utilisé pour filtrer différents types de flux :

Flux entre les utilisateurs du réseau interne et la passerelle de messagerie

La passerelle doit être placée dans la DMZ. Dans ce cas, les mails envoyés par les clients de messagerie du réseau interne à destination de la passerelle interne pourront être filtrés.

Conséquences

Le serveur de messagerie peut être déchargé des mails trop volumineux (un message d'erreur est envoyé au client de messagerie en cas de rejet d'un message), les utilisateurs internes ne peuvent pas utiliser le serveur pour faire du relaying SMTP. Votre serveur peut être protégé des HAWKs (méthode utilisée par certains virus pour se propager avec les contacts du carnet d'adresses OUTLOOK) en bloquant les messages envoyés à plusieurs destinataires simultanément.

Configuration

Activer la redirection SMTP sur le port 25 et l'interface interne.

Flux SMTP venant de la passerelle de messagerie vers l'Internet

L'IPS-Firewall est placé entre la passerelle interne et l'Internet. Les mails envoyés par la passerelle interne vers l'Internet sont filtrés.

© Copyright NETASQ 2006

Conséquences

Impossible de faire du relaying SMTP en se servant de la passerelle interne. Possibilité de limiter les envois de pièces jointes vers l'extérieur (permet d'éviter la fuite d'informations et de documents confidentiels, par exemple. Attention, les messages sont alors complètement détruits). Supprime la bannière de bienvenue du serveur SMTP.

Configuration

Activer la redirection SMTP sur le port 25 et sur l'interface sur laquelle se trouve le serveur de messagerie.

Flux SMTP venant de l'Internet vers la passerelle interne.

L'IPS-Firewall est placé entre la passerelle interne et l'Internet. Les mails reçus par la passerelle sont filtrés.

Conséquences

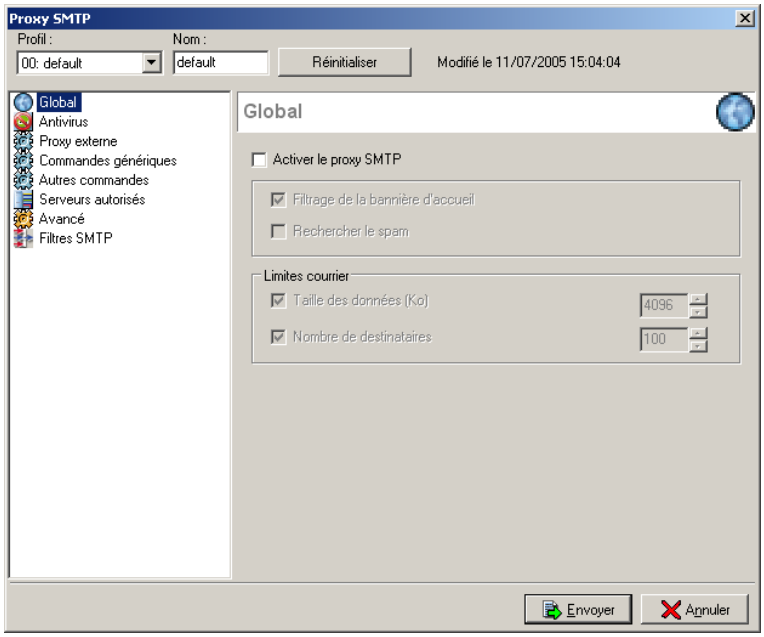
Il est possible de limiter la taille des emails entrants pour éviter une surcharge du serveur. Vous pouvez éviter le spam d'emails. Vous pouvez interdire les mails provenant de certains expéditeurs.

Configuration

Activer la redirection SMTP sur le port 25 et sur l'interface OUT.

Fonctionnement

Pour utiliser le proxy SMTP, celui-ci doit être activé. L'activation du proxy est réalisée au niveau de la section « Proxy SMTP » du menu « Proxies » de l'arborescence.



Ce menu est divisé en deux parties :

- ► A gauche un arbre présentant les diverses fonctionnalités du menu Proxy SMTP,
- ► A droite les options configurables.

Il est désormais possible de créer quatre profils pour le Proxy afin d'adapter l'analyse du proxy en fonction du sens du trafic. Cela va permettre de désactiver certaines fonctionnalités sur les trafics autorisés en sortie mais pas en entrée.

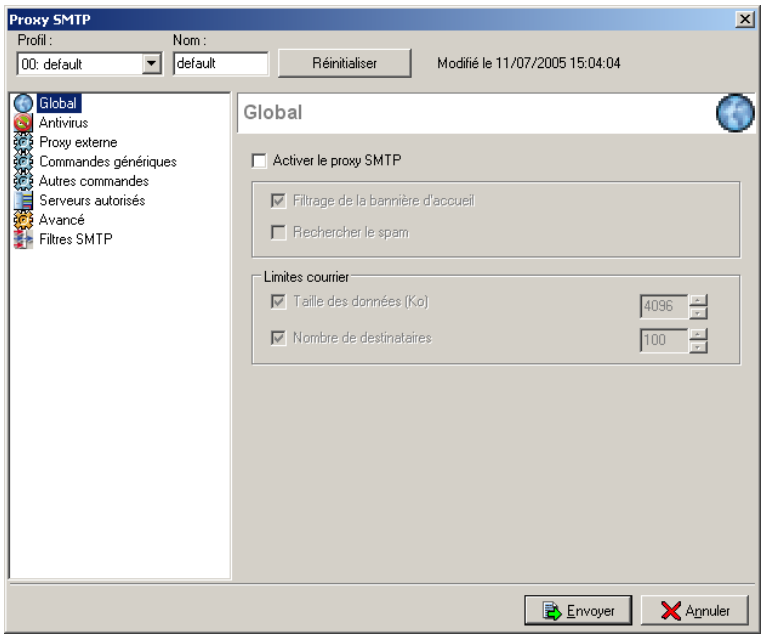
La barre d'action située en haut de l'écran vous indique quel profil du proxy SMTP est actuellement affiché. De plus vous pouvez spécifier un nom pour chacun des quatre profils.

Le bouton « Réinitialiser » vous permet de redéfinir les paramètres des profils du proxy SMTP dans leur configuration d'origine.

La date située à côté du bouton « Réinitialiser » indique la date de la dernière modification de la configuration.

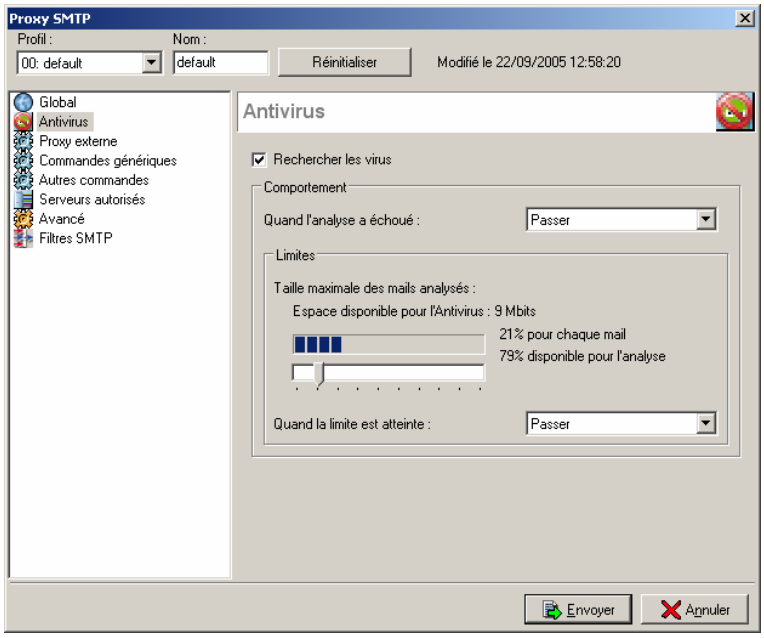
Cochez l'option « Activer le proxy SMTP » dans le menu « Global » pour activer le proxy SMTP et effectuer les analyses spécifiées dans les menus suivants.

Global



L'onglet « Global » permet de configurer les paramètres suivants :

Filtrage de la bannière d'accueil	Lorsque cette option est cochée, la bannière de votre serveur de messagerie n'est plus envoyée lors d'une connexion SMTP. En effet, cette bannière contient des informations qui peuvent être exploitées par certains pirates (type de serveur, version logicielle ...).
Recherche du spam	Activation des fonctionnalités du proxy SMTP pour la rechercher de spam.
Taille des données	Indiquez la taille maximale en Ko que peut prendre un message passant par le firewall NETASQ. Les messages dont la taille est excessive seront supprimés par le firewall (un message d'erreur est envoyé à l'expéditeur).
Nombre de destinataires	Indiquez le nombre maximum de destinataires que peut contenir un message. Les messages dont le nombre de destinataires est excessif seront supprimés par le firewall (un message d'erreur est envoyé à l'expéditeur). Permet de limiter le spam d'emails.



L'activation du proxy SMTP permet notamment l'activation de la recherche des virus dans les trafics SMTP. Pour activer la recherche des virus reportez-vous à la procédure suivante :

1. Activer le proxy SMTP en cochant l'option « Activer le proxy SMTP » dans le menu « Global » ;

2. Activer la recherche des virus en cochant l'option « Recherche des virus » dans le menu « Antivirus » ;

3. Cliquer sur OK pour valider les modifications.

Comportement

La section « Comportement » décrit le comportement de l'antivirus face à certains événements.

L'option « Lorsque l'analyse échoue » définit le comportement de l'antivirus si l'analyse du fichier qu'il est en train de scanner échoue (il ne réussit pas à analyser le fichier parce qu'il est verrouillé par exemple).

Si « Bloquer » est spécifié, le fichier en cours d'analyse n'est pas transmis.
Si « Passer » est spécifié, le fichier en cours d'analyse est transmis.

Limitation

La « Taille limite des données analysées » est fonction des capacités matérielle chaque modèle d'IPS-Firewall mais elle peut être adaptée selon les besoins de l'entreprise. Pour cela, déplacez la règlette.

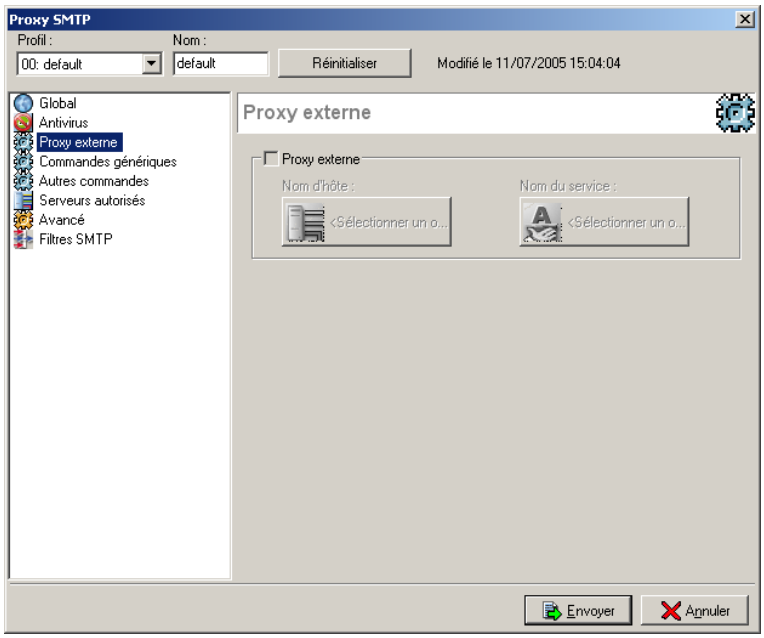
Attention lorsque vous définissez une taille limite de données analysées manuellement, veillez à conserver un ensemble de valeurs cohérentes. En effet, l'espace mémoire total, représenté par la réglette correspond à l'ensemble des ressources réservées pour le service Antivirus. Si vous définissez que la taille limite des données analysées sur SMTP est de 100% de la taille total, aucun autre fichier ne pourra être analysé en même temps.

L'option « Lorsque la limite est dépassé » définit le comportement de l'antivirus si la taille du fichier d'analyse qu'il est en train de scanner dépasse la limite autorisée.

© Copyright NETASQ 2006

Si « Bloquer » est spécifié, le fichier en cours d'analyse n'est pas transmis.
Si « Passer » est spécifié, le fichier en cours d'analyse est transmis.

Proxy externe



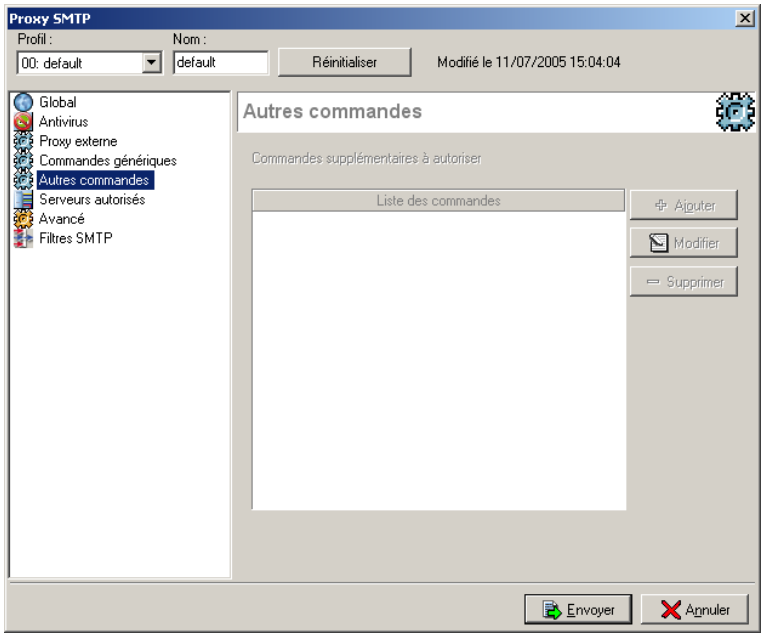
Le proxy SMTP permet de rediriger les requêtes SMTP provenant des utilisateurs du réseau interne vers des proxies externes.

Pour activer cette redirection, cochez la case correspondante puis précisez l'adresse IP du serveur ainsi que le port sur lequel il reçoit les requêtes. Si l'administrateur spécifie un groupe de serveurs dans l'option « Nom d'hôte », l'IPS-Firewall effectuera un partage de charge entre les différentes proxies externes du groupe en fonction de la machine source (une machine source donnée utilisera toujours le même proxy externe).

Commandes Génériques

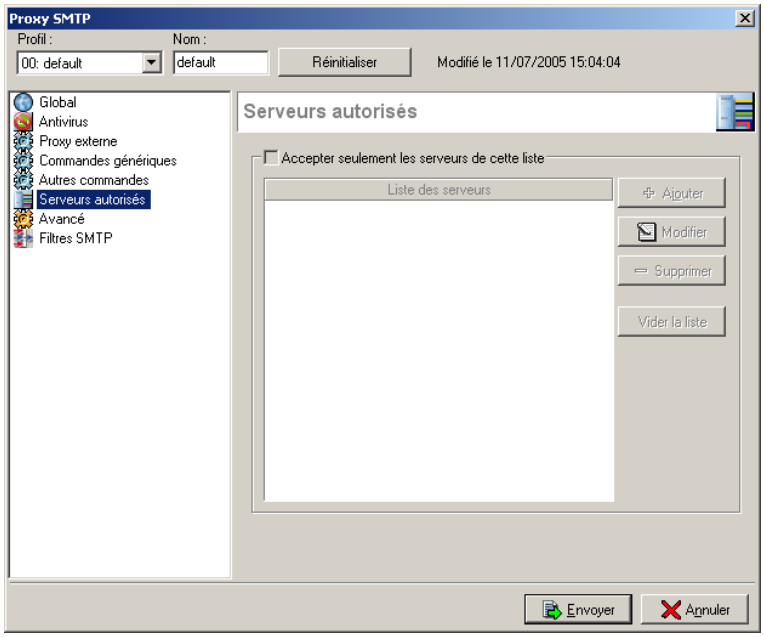
Ce menu vous permet d'autoriser ou de rejeter les commandes SMTP définies dans les RFC. Vous pouvez laisser passer une commande, la bloquer ou analyser la syntaxe et vérifier que la commande est conforme aux RFC en vigueur.

Autres commandes



Par défaut, toutes les commandes non définies dans les RFC sont interdites. Cependant, certains systèmes de messagerie utilisent des commandes supplémentaires non standardisées. Vous pouvez donc ajouter ces commandes afin de les laisser passer au travers de l'IPS-Firewall.

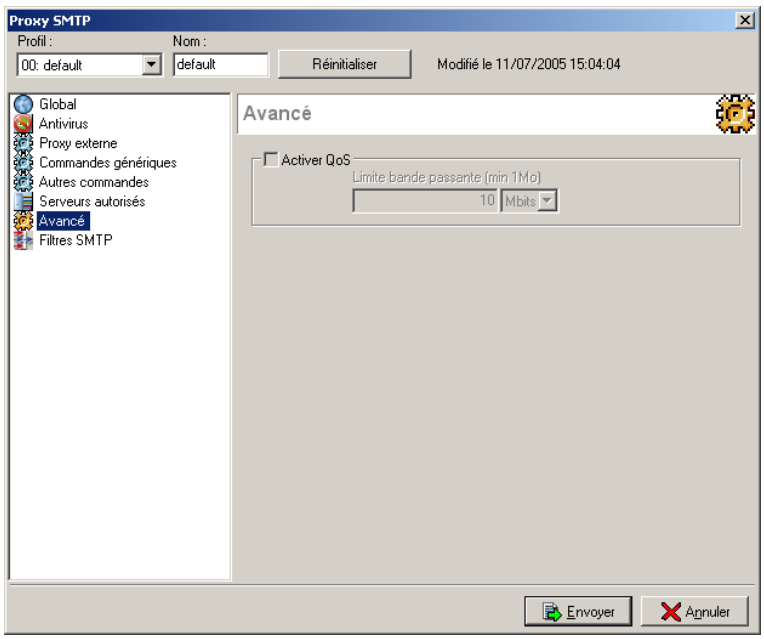
Serveurs autorisés



En sélectionnant l'option « Accepter seulement les serveurs de cette liste » vous n'autorisez le trafic SMTP qu'à destination des serveurs spécifiés dans la liste.

Les boutons d'action sur la droite de la fenêtre vous permettent de sélectionner vos serveurs autorisés dans la liste de vos objets. Les messages à destination d'un serveur ne faisant pas partie de la liste seront supprimés par le firewall. Si cette case n'est pas cochée, tous les mails sont autorisés.

Avancé

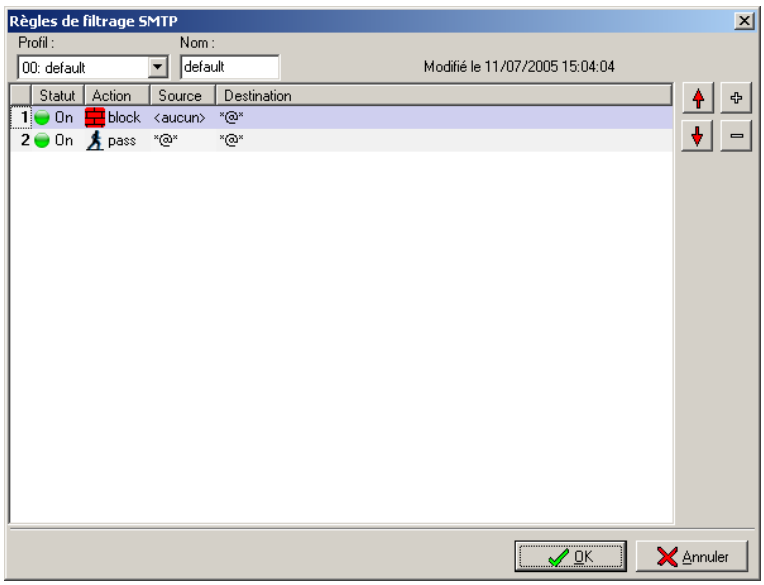


L'onglet « Avancé » permet de configurer les paramètres suivants :

Activer QoS	Régulation du trafic SMTP. Un calcul de dérivée de la courbe du trafic permet de déterminer si des paquets doivent être supprimés silencieusement afin de ne pas dépasser le débit

	limite.

Filtrage SMTP



Ce menu vous permet de réaliser un véritable filtrage sur les Emails que vous envoyez ou que vous recevez. En cliquant sur l'onglet « Filtrage SMTP » le menu de configuration apparaît. Ce menu se divise en deux parties :

- ► Une grille de définition des règles de filtrage d'Emails,
- ► Des boutons d'actions.

Boutons d'actions

Les actions réalisées par les boutons d'actions sont expliquées dans le tableau ci-dessous.

Flèche vers le haut	Placer la ligne sélectionnée avant la ligne directement au dessus.
Flèche vers le bas	Placer la ligne sélectionnée après la ligne directement en dessous.
Plus	Insérer une ligne vierge après la ligne sélectionnée.
Moins	Supprimer la ligne sélectionnée.
OK	Accepter les modifications apportées.
Annuler	Annuler les modifications apportées.

Création d'une règle de filtrage d'Emails

La grille de définition vous permet de réaliser une véritable politique de filtrage d'Emails, les colonnes de la grille représentent :

Statut	**ON** : La règle est utilisée pour le filtrage **OFF** : La règle n'est pas utilisée pour le filtrage
Action	Action réalisée par la règle de filtrage d'Emails sélectionnée.

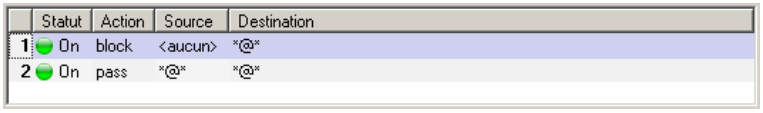
	Choisir parmi « Passer » ou « Bloquer ».
Source	Définition de l'émetteur du mail.
Destination	Définition du destinataire du mail.

La saisie d'un masque d'Emails peut comporter la syntaxe suivante :

*****	Remplace une séquence de caractères quelconque. Par exemple, *@netasq.com permet de définir l'ensemble des emails domaine Internet de la société NETASQ.
?	Remplace un caractère. Par exemple commerce ?@netasq.com est équivalent à commerce1@netasq.com ou de commercea@netasq.com mais pas à commerce12@netasq.com
[a-z]	Remplace un intervalle de caractère. Par exemple commerce[1-2]@netasq.com est équivalent à commerce1@netasq.com et à commerce2@netasq.com.
<aucun>	Cette valeur ne peut être obtenu que lorsque le champ « Source » est vide. Elle n'est utilisée que pour le cas des « Mailer Deamon ». En effet, lorsque un mail ne trouve pas de destinataire sur le serveur mail distant, un message d'erreur est renvoyé par le serveur mail distant, indiquant qu'il y a erreur sur le destinataire. Dans ce cas, le champ « Source » de ce message d'erreur est vide.

Fonctionnement des filtres SMTP et constat initial de configuration

Les filtres SMTP fonctionnent par défaut en mode « WhiteList » (ce qui n'est pas explicitement autorisé est interdit). Par défaut la configuration des filtres SMTP se compose de deux règles de filtrage SMTP.



	Statut	Action	Source	Destination
1	On	block	<aucun>	*@*
2	On	pass	*@*	*@*

La règle 1 bloque par défaut les messages des mailers démon. En effet, lorsque un mail ne trouve pas de destinataire sur le serveur mail distant, un message d'erreur est renvoyé par le serveur mail distant, indiquant qu'il y a erreur sur le destinataire. Dans ce cas, le champ « Source » de ce message d'erreur est vide. La règle 1 est une transposition explicite d'une règle existante précédemment sous une forme implicite.

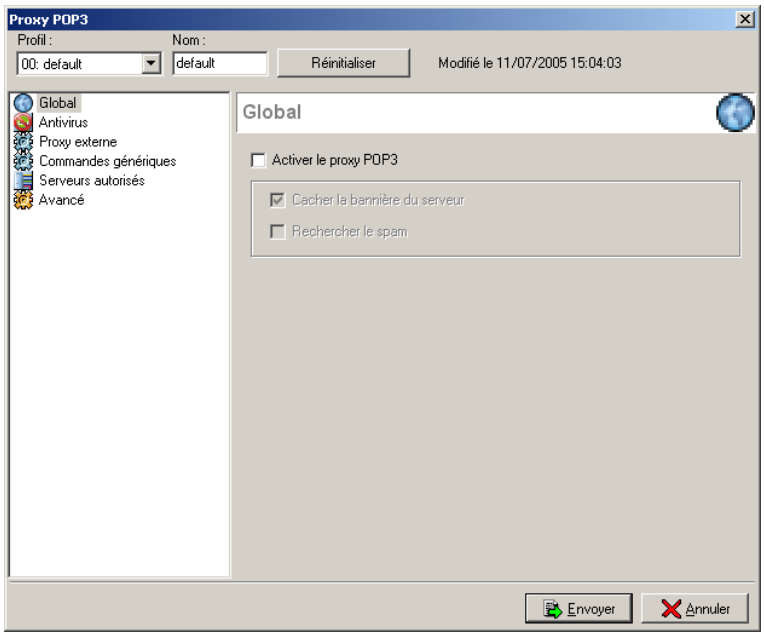
La règle 2 autorise par défaut la transmission des messages provenant de tous les expéditeurs possible à tous les destinataires possibles. Lorsque la règle 2 est supprimée et que le proxy SMTP est activé, les messages en provenance d'expéditeurs et à destination de déstinataires non autorisés sont bloqués.

Introduction

La section précédente décrit le fonctionnement et les avantages du proxy SMTP NETASQ. Comme indiqué, ce proxy est mis en place dans le cadre d'une architecture dans laquelle l'IPS-Firewall va protéger un serveur de mail interne (ou placé en DMZ) en analysant les flux SMTP et immuniser votre réseau contre la menace antivirale grâce à l'antivirus KASPERSKY intégré à l'IPS-Firewall.

Le trafic Mail n'est pas seulement basé sur le protocole SMTP mais aussi sur POP3. Ce protocole va permettre à l'utilisateur d'un logiciel de messagerie, de récupérer sur son poste, des mails, stockés sur un serveur distant. Ce serveur de mail distant pouvant être situé à l'extérieur du réseau local ou sur une interface distincte, le flux POP3 transite au travers de l'IPS-Firewall lui permettant de réaliser son analyse.

Fonctionnement



Pour utiliser le proxy POP3, celui-ci doit être activé. L'activation du proxy est réalisée au niveau de la section « Proxy POP3 » du menu « Proxies » de l'arborescence.

Ce menu est divisé en deux parties :

- ► A gauche un arbre présentant les diverses fonctionnalités du menu Proxy POP3,
- ► A droite les options configurables.

Il est possible de créer quatre profils pour le Proxy afin d'adapter l'analyse du proxy en fonction du sens du trafic. Cela va permettre de désactiver certaines fonctionnalités sur les trafics autorisés en sortie mais pas en entrée.

La barre d'action située en haut de l'écran vous indique quel profil du proxy POP3 est actuellement affiché. De plus vous pouvez spécifier un nom pour chacun des quatre profils.

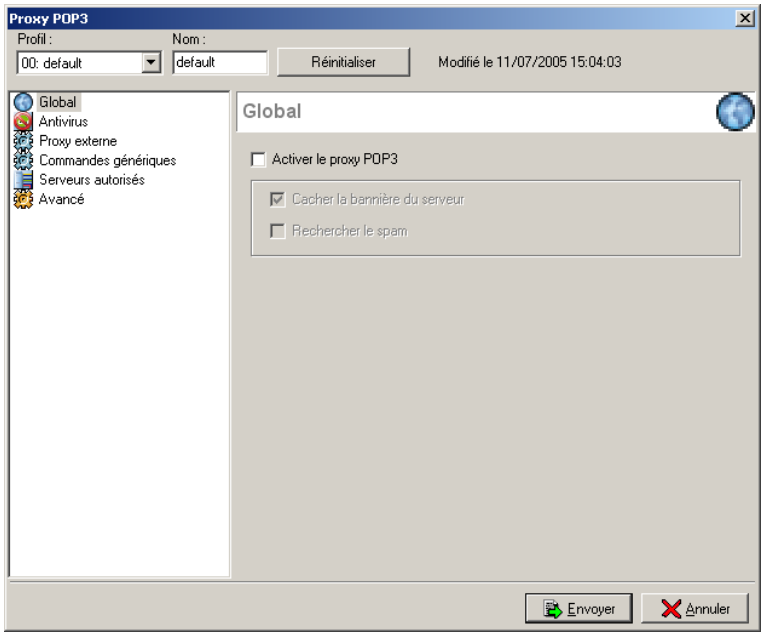
© Copyright NETASQ 2006

Le bouton « Réinitialiser » vous permet de redéfinir les paramètres des profils du proxy POP3 dans leur configuration d'origine.

La date située à côté du bouton « Réinitialiser » indique la date de la dernière modification de la configuration.

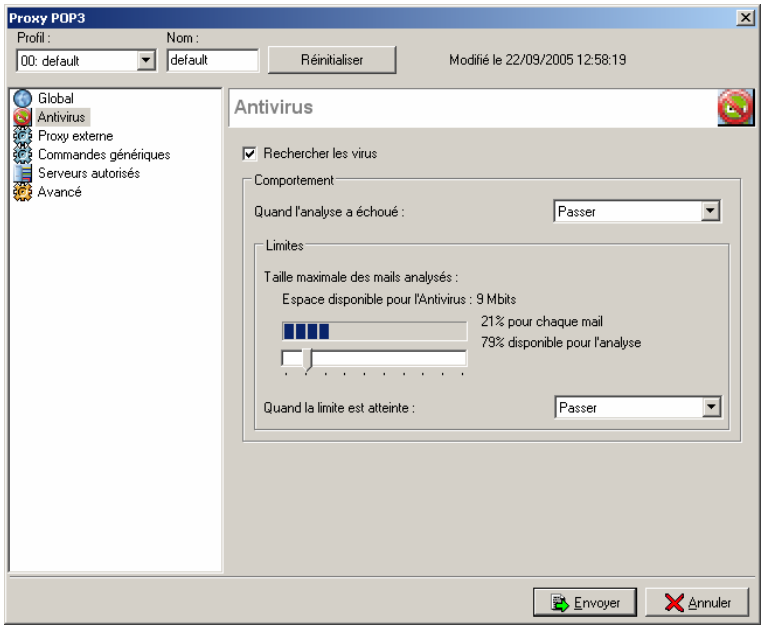
Cochez l'option « Activer le proxy POP3 » dans le menu « Global » pour activer le proxy POP3et effectuer les analyses spécifiées dans les menus suivants.

Global



L'onglet « Global » permet de configurer les paramètres suivants :

Filtrage de la bannière d'accueil	Lorsque cette option est cochée, la bannière de votre serveur de messagerie n'est plus envoyée lors d'une connexion POP3. En effet, cette bannière contient des informations qui peuvent être exploitées par certains pirates (type de serveur, version logicielle ...).
Recherche du spam	Activation des fonctionnalités du proxy POP3 pour la rechercher de spam.



L'activation du proxy POP3 permet notamment l'activation de la recherche des virus dans les trafics POP3. Pour activer la recherche des virus reportez-vous à la procédure suivante :

1. Activer le proxy POP3 en cochant l'option « Activer le proxy POP3 » dans le menu « Global » ;

2. Activer la recherche des virus en cochant l'option « Recherche des virus » dans le menu « Antivirus » ;

3. Cliquer sur OK pour valider les modifications.

Comportement

La section « Comportement » décrit le comportement de l'antivirus face à certains événements.

L'option « Lorsque l'analyse échoue » définit le comportement de l'antivirus si l'analyse du fichier qu'il est en train de scanner échoue (il ne réussit pas à analyser le fichier parce qu'il est verrouillé par exemple).

Si « Bloquer » est spécifié, le fichier en cours d'analyse n'est pas transmis.
Si « Passer » est spécifié, le fichier en cours d'analyse est transmis.

Limitation

La « Taille limite des données analysées » est fonction des capacités matérielle chaque modèle d'IPS-Firewall mais elle peut être adaptée selon les besoins de l'entreprise. Pour cela, déplacez la règlette.

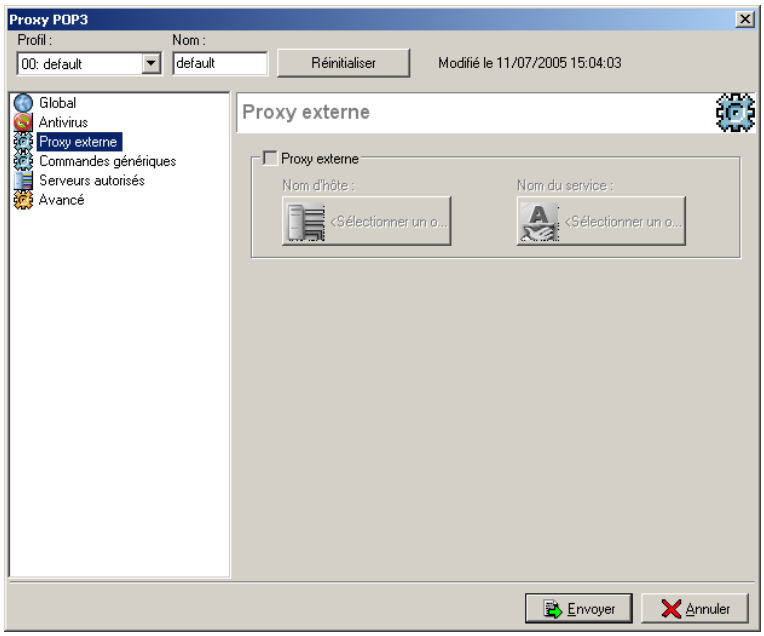
Attention lorsque vous définissez une taille limite de données analysées manuellement, veillez à conserver un ensemble de valeurs cohérentes. En effet, l'espace mémoire total, représenté par la réglette correspond à l'ensemble des ressources réservées pour le service Antivirus. Si vous définissez que la taille limite des données analysées sur POP3 est de 100% de la taille total, aucun autre fichier ne pourra être analysé en même temps.

L'option « Lorsque la limite est dépassé » définit le comportement de l'antivirus si la taille du fichier d'analyse qu'il est en train de scanner dépasse la limite autorisée.

© Copyright NETASQ 2006

Si « Bloquer » est spécifié, le fichier en cours d'analyse n'est pas transmis.
Si « Passer » est spécifié, le fichier en cours d'analyse est transmis.

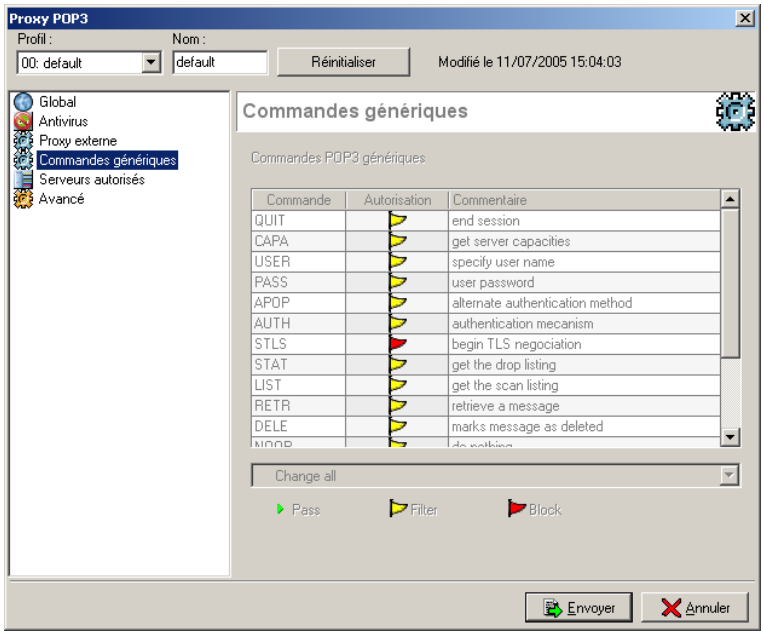
Proxy externe



Le proxy POP3 permet de rediriger les requêtes POP3 provenant des utilisateurs du réseau interne vers des proxies externes.

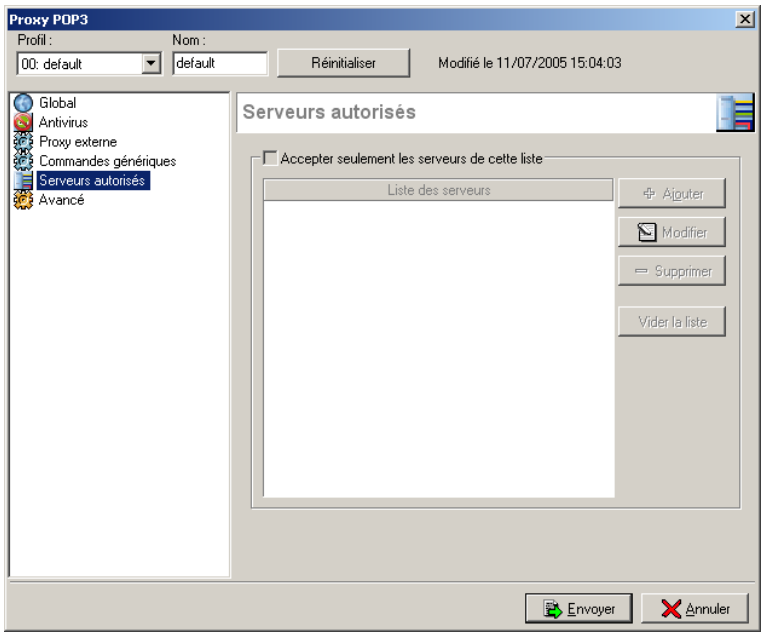
Pour activer cette redirection, cochez la case correspondante puis précisez l'adresse IP du serveur ainsi que le port sur lequel il reçoit les requêtes.

Commandes Génériques



Ce menu vous permet d'autoriser ou de rejeter les commandes POP3 définies dans les RFC. Vous pouvez laisser passer une commande, la bloquer ou analyser la syntaxe et vérifier que la commande est conforme aux RFC en vigueur.

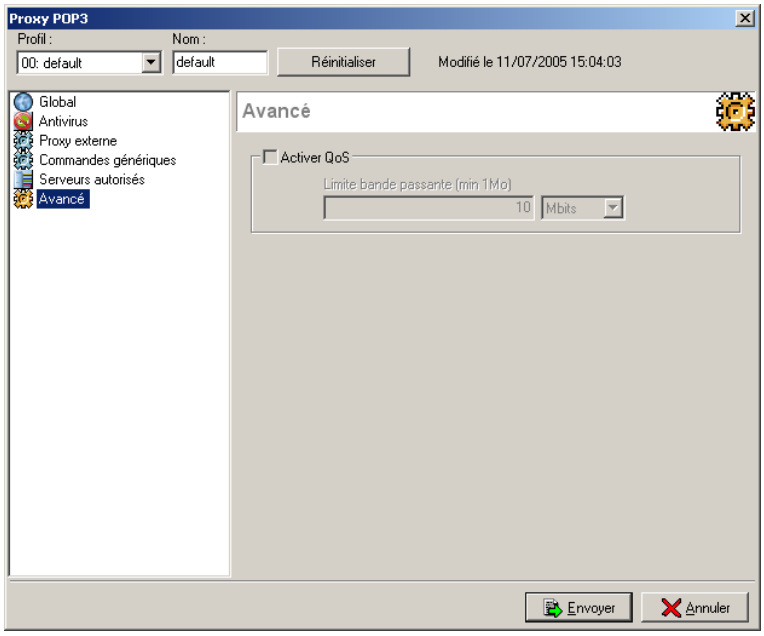
Serveurs autorisés



En sélectionnant l'option « Accepter seulement les serveurs de cette liste » vous n'autorisez le trafic POP3 qu'à destination des serveurs spécifiés dans la liste.

Les boutons d'action sur la droite de la fenêtre vous permettent de sélectionner vos serveurs autorisés dans la liste de vos objets. Les messages à destination d'un serveur ne faisant pas partie de la liste seront supprimés par le firewall. Si cette case n'est pas cochée, tous les mails sont autorisés.

Avancé



L'onglet « Avancé » permet de configurer les paramètres suivants :

Activer QoS	Régulation du trafic POP3. Un calcul de dérivée de la courbe du trafic permet de déterminer si des paquets doivent être supprimés silencieusement afin de ne pas dépasser le débit limite.

Section B

Filtrage de contenu

© Copyright NETASQ 2006

Pour cette section, vous devez avoir franchi les étapes

► Installation, pré-configuration, intégration,
► Définition des interfaces, des objets et de la configuration du noyau,
► Proxies HTTP, SMTP et POP3.

Pour cette section, vous devez connaître

► La politique de filtrage URL de l'entreprise,
► Les adresses des différents proxies.

Utilité de la section

Cette section vous permet de définir les règles de filtrage URL que vous allez appliquer aux postes.

Accéder à cette section

Accédez à la boîte de dialogue par le sous-menu « Analyse de contenu > Filtrage d'URLs ».

Vous devez être connecté avec les privilèges de modification pour pouvoir effectuer ces modifications. Avant d'effectuer toute modification importante sur votre Firewall NETASQ, nous vous conseillons d'effectuer une sauvegarde. Ainsi, en cas de mauvaise manipulation vous pourrez vous retrouver dans l'état précédent. Pour plus d'informations sur les sauvegardes, veuillez vous référer au chapitre adéquat. (Voir « Sauvegarde et mise à jour »).

Introduction à cette section

Vous pouvez imposer l'authentification pour le filtrage d'URLs. Lorsqu'un utilisateur voudra accéder au WEB ou à certains sites WEB, il devra alors s'authentifier. Lorsque le filtrage d'URLs est actif et que l'utilisateur doit s'authentifier, une page d'authentification est proposée à ce dernier lors de la consultation d'un site WEB.

Les tables de filtrage URL sont stockées sur le Firewall NETASQ dans des slots (fichiers de configuration numérotés de 01 à 10). Chaque slot peut être programmé à une heure précise de la semaine, en écrasant la configuration du slot précédemment activée. (Voir « Programmation des slots »).

© Copyright NETASQ 2006

Introduction

Le développement exceptionnel d'Internet et la banalisation de l'utilisation de l'email ont favorisé l'émergement de ce qu'on appelle « le spam ». Ces courriers électroniques indésirables, vantant les mérites de produits ou services, polluent encore et toujours les boîtes aux lettres électroniques des utilisateurs de messageries WEB.

De plus, en recherche constante de nouvelles techniques de spams, les spammeurs déjouent une à une les contre-mesures mises en place par les administrateurs pour protéger les boîtes aux lettres de leurs utilisateurs. Ainsi les nouvelles contre-mesures se doivent de multiplier les méthodes d'analyse pour gérer des spams aussi variés et variables que possibles.

Le module antispam intégré par NETASQ dans ses appliances UTM est basé sur 4 méthodes d'analyse complémentaires: une analyse par liste noire DNS, une analyse heuristique, un filtrage par liste noire de domaines et un filtrage par liste blanche de domaines.

L'analyse par liste noire DNS ou RBL DNS

L'analyse par liste noire DNS ou RBL (« Realtime Blackhole List ») permet la qualification d'un message en spam par l'intermédiaire de serveurs RBL. Ces serveurs RBL contiennent des listes d'adresses IP identifiant les spammeurs et tous les serveurs qui relayent le spam sans le combattre.

Pour chaque message à analyser, l'appliance UTM demande auprès de ces serveurs RBL si l'expéditeur ou les relais de messagerie par lesquels le message a transité est considéré comme un spammeur. Puis l'appliance UTM se base sur leur réponse pour qualifier le message comme un spam.

L'analyse heuristique ou bayésienne

L'analyse heuristique est basée sur l'antispam VadeRetro de GOTO Software. Cet antispam utilise de 7 méthodes d'analyse pour évaluer la légitimité d'un mail analysé.

Analyse par règles empiriques
L'analyse par règles empiriques est basée sur l'utilisation de règles, non prédictibles, déduites à partir de l'analyse approfondie de tous les composants du message (champs d'entête, texte du sujet, corps du texte, html, pièces jointes,...). Ces règles, déterminées par les experts Vaderetro, définissent un ensemble de caractéristiques originales, communes à certains types de messages (comme par exemple les messages envoyés par des robots). Elles permettent ainsi de repérer de futures messages qui posséderaient les mêmes caractéristiques.

Analyse sémantique
L'analyse sémantique consiste à comparer le contenu textuel du message à un dictionnaire prédéfini de mots et locutions caractéristiques des spams ou des messages légitimes. La technologie de recherche de locution de VadeRetro est aussi originale dans son approche, puisqu'elle permet de rechercher des combinaisons logiques de mots mais aussi de détecter des mots avec une orthographe approchante.

Recherche de contre-mesures
Les filtres de ce type constituent sans doute la partie le plus originale et la plus efficace du moteur de filtrage VadeRetro. Ils consistent à détecter, dans les messages, les techniques qu'emploient les spammeurs pour déjouer les solutions anti-spams utilisant les méthodes de filtrage « classiques ».

Analyse du code HTML intégré
Lorsque le message contient une partie HTML, une « empreinte » de ce code est établie par l'antispam. Cette empreinte est alors comparée à une liste « d'empreintes » couramment utilisées par les spammeurs. Cette méthode, associée à une technique de statistiques sur les tailles

© Copyright NETASQ 2006

d'images, permet d'identifier, entre autres, certains messages indésirables qui ne contiennent pas de texte, mais seulement une ou plusieurs images.

Recherche de langues étrangères non latines
L'apparition de plus en plus courante de spams en provenance de l'Asie ou des pays de l'Est rend désormais indispensable l'identification des jeux de caractères non latin. Cela soit lors de la déclaration du jeu de caractères soit lors de son utilisation effective.

Analyse Anti-Scams
Les scams sont des escroqueries qui reposent le plus souvent sur des propositions de participation à une opération financière internationale très alléchante. Initialement pratiqués par courrier traditionnel ou par fax, les scams ont aujourd'hui leur déclinaison par e-mail sous forme de spams qui ne ressemblent pas aux autres messages publicitaires habituellement filtrés. La technologie VadeRetro inclut un module spécifique de détection des messages de ce type.

Détection des notifications d'antivirus et de non remise
Les serveurs de messagerie sont actuellement engorgés par les messages de notification induits par la prolifération des virus par e-mail. En effet, ce type de virus exploitent les carnets d'adresses des machines infectées et envoient des messages en falsifiant l'adresse de l'émetteur. Le filtrage de VadeRetro comporte un module spécifique d'identification des divers messages de notification émis par les serveurs SMTP lors de la détection d'un virus ou de la non remise d'un message à une adresse e-mail inexistante.

Filtrage par liste noire de domaines

Les deux premières analyses très évoluées du module Antispam NETASQ sont complétés par des filtres basiques de domaines. Le filtrage par liste noire de domaines contient la liste des domaines qui doivent être systématiquement considéré comme spammeurs.

Filtrage par liste blanche de domaines

Le filtrage par liste blanche de domaines définit que contient la liste des domaines qui doivent être systématiquement considéré comme légitimes.

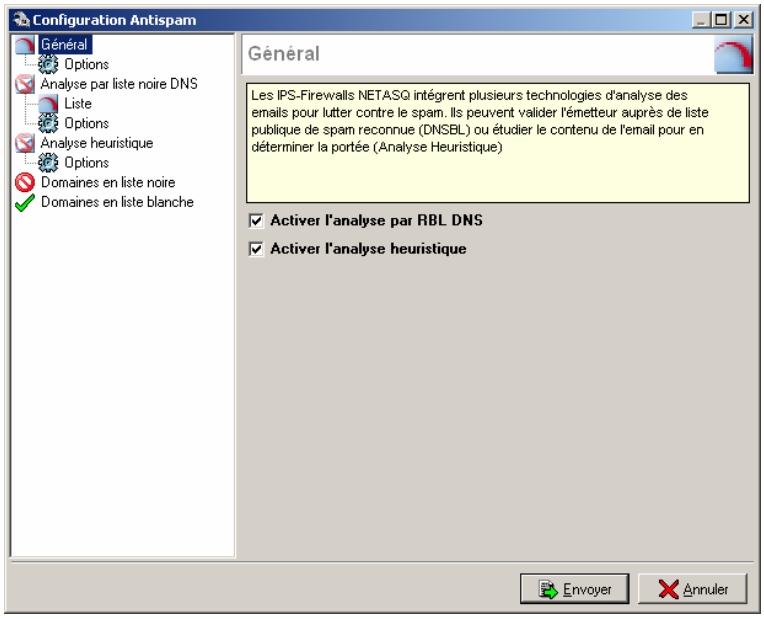
Utilisation possible de l'antispam des IPS-Firewalls NETASQ

L'antispam permet de marquer les emails lorsqu'ils correspondent à du spam. Ainsi il est alors possible de classer automatiquement ces mails grâce aux fonctions de « rangement » de votre client de messagerie. NETASQ conseille de réaliser des filtres de vos mails et de placer un filtre spécial correspondant au spam à la toute fin de vos filtres. Ainsi si un de vos mails valide est tout de même marqué comme du spam, il est rangé par vos filtres personnels avant d'être traité par le filtre du spam.

Notez que le module Antispam détermine un niveau de confiance (de 1 à 3) qui définit un niveau de certitude qu'a le module Antispam d'avoir détecté un spam (1 pour peu confiant, 3 pour très confiant). Ce niveau de confiance se retrouve dans la configuration notamment des serveurs RBL.

Fonctionnement

Pour utiliser l'antispam des IPS-Firewalls NETASQ, celui-ci doit être activé. L'activation du service est réalisée au niveau du menu « Analyse de contenu > Antispam » de l'arborescence.


Configuration Antispam
Général
Options
Analyse par liste noire DNS
Liste
Options
Analyse heuristique
Options
Domaines en liste noire
Domaines en liste blanche
Général
Les IPS-Firewalls NETASQ intégrent plusieurs technologies d'analyse des emails pour lutter contre le spam. Ils peuvent valider l'émetteur auprès de liste publique de spam reconnue (DNSBL) ou étudier le contenu de l'email pour en déterminer la portée (Analyse Heuristique)
Activer l'analyse par RBL DNS
Activer l'analyse heuristique
Envoyer
Annuler

Le proxy DNS doit être activé pour le fonctionnement de l'antispam.

L'écran de configuration du service Antispam se décompose en deux parties :

► A gauche un arbre présentant les diverses fonctionnalités du menu Service Antispam,
► A droite les options configurables.

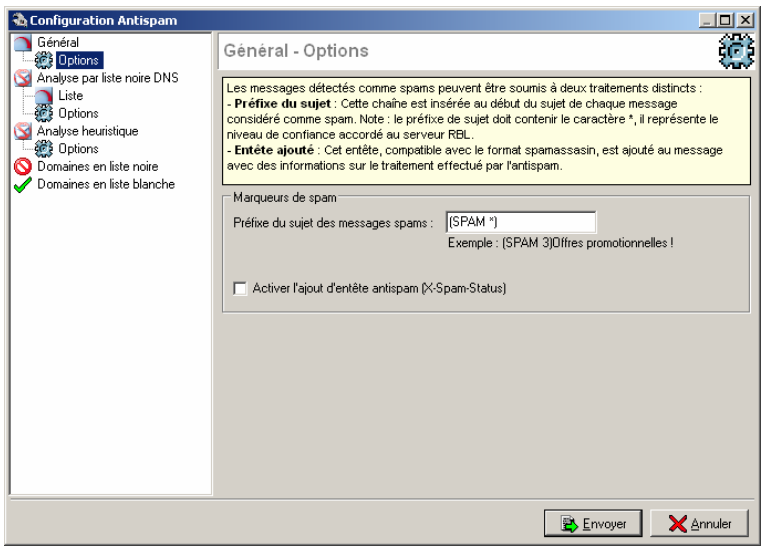
Les boutons « Envoyer » et « Annuler » situés dans le coin inférieur droit permettent respectivement l'application des modifications effectuées sur la configuration et l'annulation des modifications.

Général

L'activation de l'antispam s'effectue en déterminant qu'elles seront les analyses activées. Deux choix sont disponibles :

► L'analyse par RBL DNS : pour activer l'analyse par liste noire DNS,
► L'analyse heuristique : pour activer le module Antispam VadeRetro.

Options


Configuration Antispam
Général
Options
Analyse par liste noire DNS
Liste
Options
Analyse heuristique
Options
Domaines en liste noire
Domaines en liste blanche
Général - Options
Les messages détectés comme spams peuvent être soumis à deux traitements distincts :
- Préfixe du sujet : Cette chaîne est insérée au début du sujet de chaque message considéré comme spam. Note : le préfixe de sujet doit contenir le caractère *, il représente le niveau de confiance accordé au serveur RBL.
- Entête ajouté : Cet entête, compatible avec le format spamassasin, est ajouté au message avec des informations sur le traitement effectué par l'antispam.
Marqueurs de spam
Préfixe du sujet des messages spams :
(SPAM *)
Exemple : (SPAM 3)Offres promotionnelles !
Activer l'ajout d'entête antispam (X-Spam-Status)
Envoyer
Annuler

Les messages identifiés comme spam ne sont pas supprimés par le module Antispam de l'appliance UTM NETASQ. Cependant il effectue des actions de modifications du message détecté

comme spam de façon à permettre un traitement futur par le client de messagerie WEB par exemple. Deux actions de marquage sont disponibles :

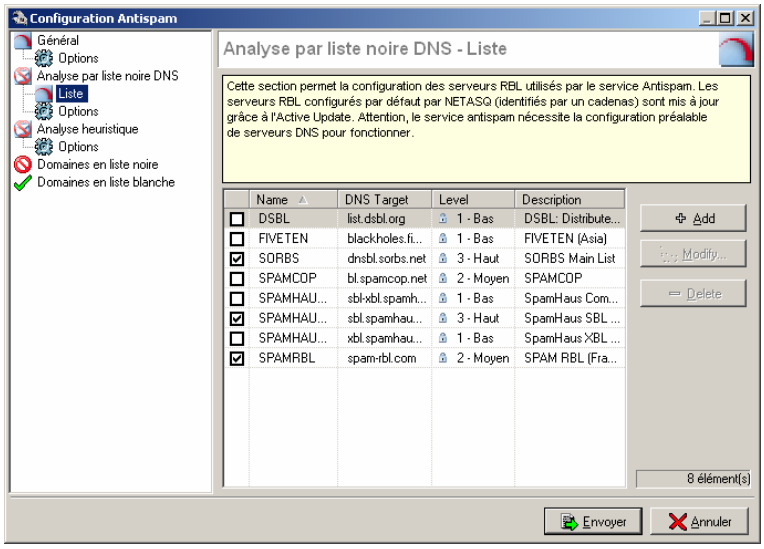
► Préfixe du sujet des messages spams : Le sujet des messages identifiés comme spam sont préfixés par la chaine de caractères définies. Par défaut cette chaîne est (SPAM *) où « * » représente le niveau de confiance accordé. Quelle que soit la chaîne de caractères utilisée, il est indispensable de prévoir l'insertion du niveau de confiance dans cette chaîne en utilisant « * »,

► L'entête antispam : lorsque l'option « Activer l'ajout d'entête Antispam » est cochée, le module Antispam ajoute au message identifié comme spam, un entête synthétisant le résultat de son analyse pour ce message. Cet entête antispam, au format « spamassassin » peut ensuite être utilisé par le client de messagerie WEB pour effectuer les traitements adéquats sur le message marqué.

Analyse par liste noire DNS ou RBL DNS

L'analyse par liste noire DNS ou RBL (« Realtime Blackhole List ») permet la qualification d'un message en spam par l'intermédiaire de serveurs RBL. Les menus suivant permettent de configurer la liste des serveurs RBL qui seront utilisés pour cette analyse ainsi que le niveau de confiance accordé à chacun des serveurs.

Liste


Configuration Antispam
Général
Options
Analyse par liste noire DNS
Liste
Options
Analyse heuristique
Options
Domaines en liste noire
Domaines en liste blanche
Analyse par liste noire DNS - Liste
Cette section permet la configuration des serveurs RBL utilisés par le service Antispam. Les serveurs RBL configurés par défaut par NETASQ (identifiés par un cadenas) sont mis à jour grâce à l'Active Update. Attention, le service antispam nécessite la configuration préalable de serveurs DNS pour fonctionner.
Name
DNS Target
Level
Description
DSBL list.dsbl.org 1 - Bas DSBL: Distribute...
FIVETEN blackholes.fi... 1 - Bas FIVETEN (Asia)
SORBS dnsbl.sorbs.net 3 - Haut SORBS Main List
SPAMCOP bl.spamcop.net 2 - Moyen SPAMCOP
SPAMHAU... sbl-xbl.spamh... 1 - Bas SpamHaus Com...
SPAMHAU... sbl.spamhau... 3 - Haut SpamHaus SBL ...
SPAMHAU... xbl.spamhau... 1 - Bas SpamHaus XBL ...
SPAMRBL spam-rbl.com 2 - Moyen SPAM RBL (Fra...
Add
Modify...
Delete
8 élément(s)
Envoyer
Annuler

Dans cette section, une grille affiche une liste des serveurs RBL auxquels l'appliance UTM envoie ses requêtes pour vérifier qu'un email n'est pas un spam. Cette liste est actualisée par l'Active Update. Elle n'est pas modifiable mais vous pouvez toutefois désactiver certains serveurs en cliquant sur la case présente au début de chaque ligne.

Le niveau spécifié dans les colonnes de la grille indique le niveau de confiance accordé à ce serveur.

Vous pouvez aussi configurer vos propres serveurs RBL auxquels vous souhaitez que l'appliance se connecte. Pour ajouter un serveur, cliquez sur le bouton « Ajouter », spécifier alors un nom pour ce serveur, un domaine ciblé (nom DNS uniquement), un niveau de confiance et enfin un commentaire.

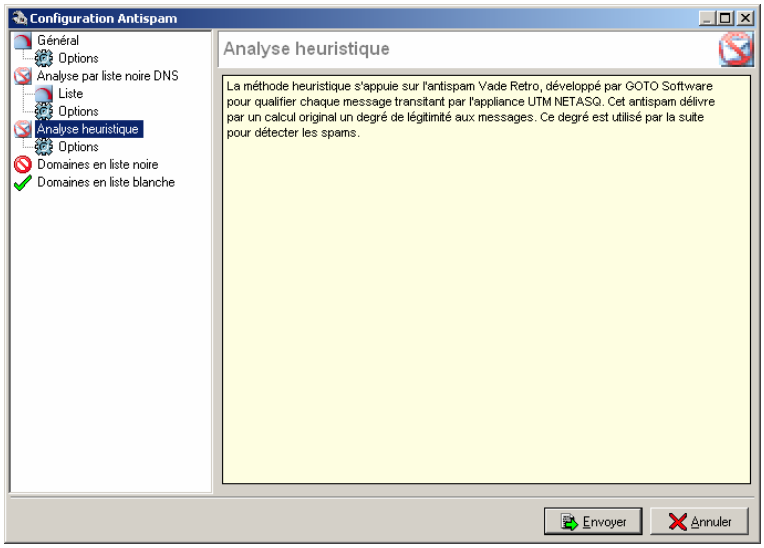
Pour supprimer ou modifier un serveur configuré, cliquez respectivement sur les boutons « Supprimer » et « Modifier ».

Notez que la différenciation entre les serveurs RBL nativement configurés par NETASQ et les serveurs configurés de manière personnalisée s'effectue grâce au cadenas « » qui indique les serveur RBL nativement configurés par NETASQ. Rappel seule la liste de ces serveurs est mise à jour par Active Update.

Options

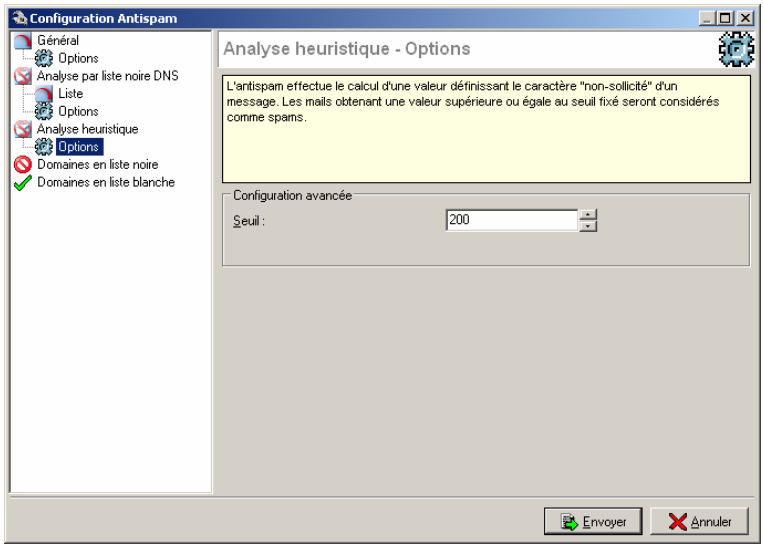
Le serveur local SMTP désigne le nom canonique de votre serveur SMTP. Cette information est facultative, si elle est renseignée, le module antispam analysera plus finement les mails relayés par de multiples serveurs.

Analyse heuristique


Configuration Antispam
Général
Options
Analyse par liste noire DNS
Liste
Options
Analyse heuristique
Options
Domaines en liste noire
Domaines en liste blanche
Analyse heuristique
La méthode heuristique s'appuie sur l'antispam Vade Retro, développé par GOTO Software pour qualifier chaque message transitant par l'appliance UTM NETASQ. Cet antispam délivre par un calcul original un degré de légitimité aux messages. Ce degré est utilisé par la suite pour détecter les spams.
Envoyer
Annuler

L'analyse heuristique est basée sur l'antispam VadeRetro de GOTO Software. La configuration de l'analyse effectuée par VadeRetro s'effectue dans la section « Options » du menu de l'analyse heuristique.

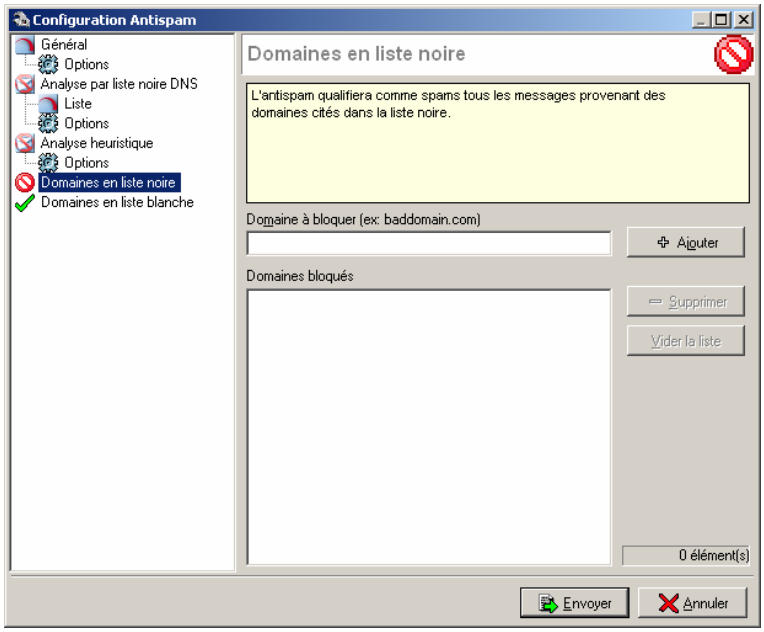
Options



L'analyse heuristique effectuée par le module Antispam effectue le calcul d'une valeur définissant le caractère « non-sollicité » d'un message. Les mails obtenant une valeur supérieure ou égale au seuil fixé seront considérés comme spams. Cette section permet de définir le seuil à appliquer, par défaut NETASQ choisit 200.

De plus, plus cette valeur calculée est élevée plus le niveau de confiance accordé par l'antispam à l'analyse sera élevé. Les seuils de franchissement des niveaux de confiance ne sont pas configurables dans le Firewall Manager.

Domaines en liste noire

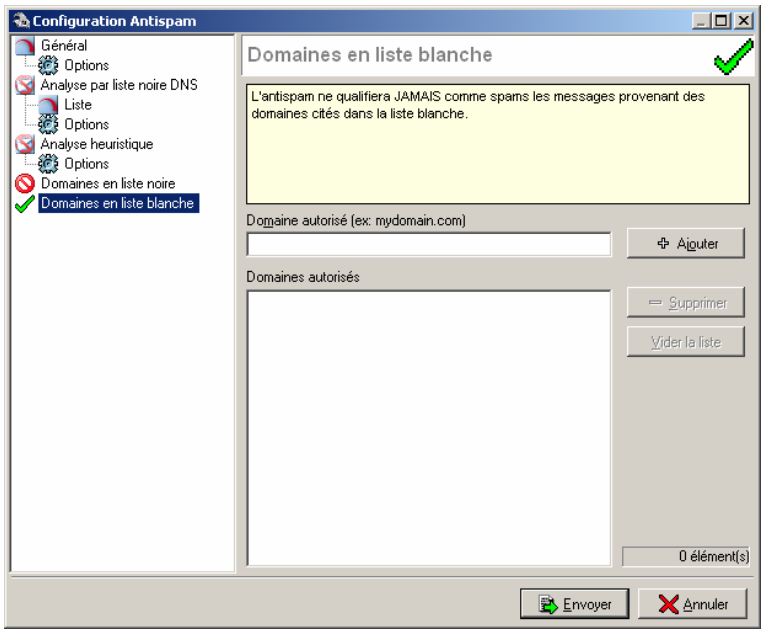


Cette section permet de définir les domaines en provenance desquels les messages analysés seront systématiquement définis comme spams. Pour ajouter un domaine à bloquer, reportez-vous à la procédure suivante :

► Spécifier le domaine à bloquer sous l'intitulé « Domaine à bloquer (ex mauvaisdomaine.com) »,
► Cliquer sur Ajouter.

Le domaine ainsi ajouté apparaît alors dans la liste des domaines en liste noire. Chaque message identifié comme spam du fait de ces domaines en liste noire seront associés au niveau de confiance le plus élevé (à savoir 3). Pour supprimer un domaine donné ou la liste complète des domaines, cliquez respectivement sur « Supprimer » et « Vider la liste ».

Domaines en liste blanche



Cette section permet de définir les domaines en provenance desquels les messages analysés seront systématiquement définis comme **légitimes**. Pour ajouter un domaine à autoriser, reportez-vous à la procédure suivante :

► Spécifier le domaine à autoriser sous l'intitulé « Domaine à autoriser (ex bondomaine.com) »,

► Cliquer sur Ajouter.

Le domaine ainsi ajouté apparaît alors dans la liste des domaines en liste blanche. Pour supprimer un domaine donné ou la liste complète des domaines, cliquez respectivement sur « Supprimer » et « Vider la liste ».

De part sa position centrale sur votre réseau, l'IPS-Firewall NETASQ est un élément important de la politique de sécurité de votre entreprise. En tant que passerelle indispensable en direction et vers l'Internet, votre IPS-Firewall vous protège contre les intrusions grâce notamment à son moteur de prévention et de détection d'intrusion l'ASQ.

Cette protection contre les intrusions est associée à un service Antivirus pemettrant le filtrage du contenu des trafics transitant au travers de l'IPS-Firewall à la recherche de virus, portes dérobées (backdoor), chevaux de Troie (trojan) ou autres malwares que l'on rencontrer sur Internet.

L'offre de service Antivirus sur les IPS-Firewalls NETASQ se compose de deux solutions.

Le service antivirus ClamAV

Projet « Open-source » l'antivirus ClamAV est intégré gratuitement et par défaut dans les produits IPS-Firewalls NETASQ. Il offre ainsi une protection contre les virus et complète l'offre de protection tout en un des IPS-Firewalls NETASQ.

Démon multi-threadé (il peut effectuer plusieurs tâches simultanément) rapide, flexible et extensible, il est une solution performante aux problèmes causés par les virus circulant sur Internet. Disposant d'une base d'environ 36 000 signatures de virus, vers et Chevaux de troie, il offre une bonne protection qui se complète de jour en jour.

Le service antivirus Kaspersky

Kaspersky Labs est un éditeur international de logiciels antivirus, anti-hacker et contre le spamming fondé en 1997.

Grâce à un dur travail et à une profonde implication, Kaspersky Labs est devenu un leader en matière de développement de systèmes de défense antivirus. Kaspersky Labs a été le premier à développer de nombreux standards de technologie dans l'industrie de l'antivirus, y compris des solutions de grande envergure pour Linux, Unix et NetWare, un analyseur heuristique de seconde génération conçu pour détecter les virus encore inconnus, un système de défense efficace contre les virus polymorphes et géants, une base de données antivirus mise à jour régulièrement **(elle dispose actuellement de plus de 120 000 signatures)** et la capacité de rechercher des virus dans les fichiers d'archive.

Le service antivirus Kaspersky n'est disponible que par l'intermédiaire d'une mise à jour payante de l'IPS-Firewall. Pour plus d'informations sur le service antivirus Kaspersky, veuillez contacter votre partenaire.

Attention, NETASQ vous met en garde !

Attention, la mise en place du service Antivirus du firewall NETASQ n'apporte pas une solution globale aux problèmes que posent les virus.

© Copyright NETASQ 2006

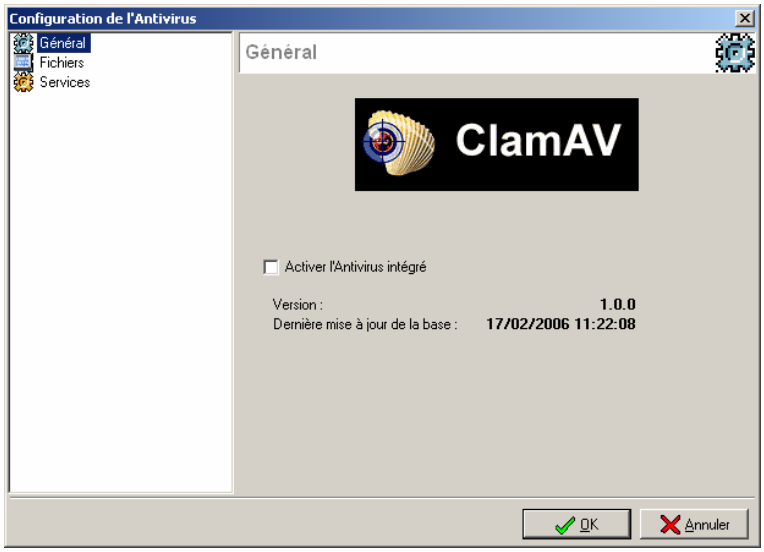
Il est INDISPENSABLE de mettre en place une solution qui analyse les postes de travail et serveurs pour protéger vos ressources réseau contre l'insertion de virus par des voies telles que les systèmes physiques de transport de données (disquettes, …).

Utilisation possible du service Antivirus du firewall NETASQ

En complément du filtrage effectué par les proxies SMTP, POP3 et HTTP (Activation préalable des proxies pour l'utilisation du service Antivirus), le service Antivirus vous protège des virus se cachant dans le flux de données SMTP, POP3 et HTTP.

Le service antivirus ne fonctionne que sur les interfaces sur lesquelles les proxies SMTP, POP3 et HTTP ont été activés. Dans le cas où vous désirez protéger votre réseau contre les virus provenant d'un trafic SMTP externe, il est nécessaire d'activer le proxy SMTP en ce sens (Chapitre V, Section A, Proxies HTTP, SMTP et POP3**).**

Fonctionnement



Pour utiliser le service Antivirus, celui-ci doit être activé. L'activation du service est réalisée au niveau du menu « Analyse de contenu > Antivirus » de l'arborescence.

L'écran de configuration du service Antivirus se décompose en deux parties :

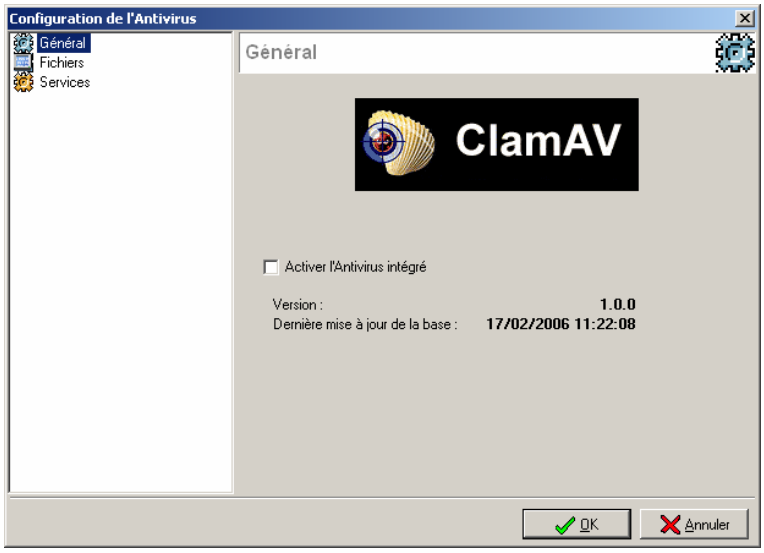
- ► A gauche un arbre présentant les diverses fonctionnalités du menu Service Antivirus,
- ► A droite les options configurables.

L'activation du service Antivirus d'un IPS-Firewall NETASQ nécessite certaines opérations préalables :

1. Activation des proxies (Chapitre V Section A),
2. Puis activation de l'antivirus.

© Copyright NETASQ 2006

Général

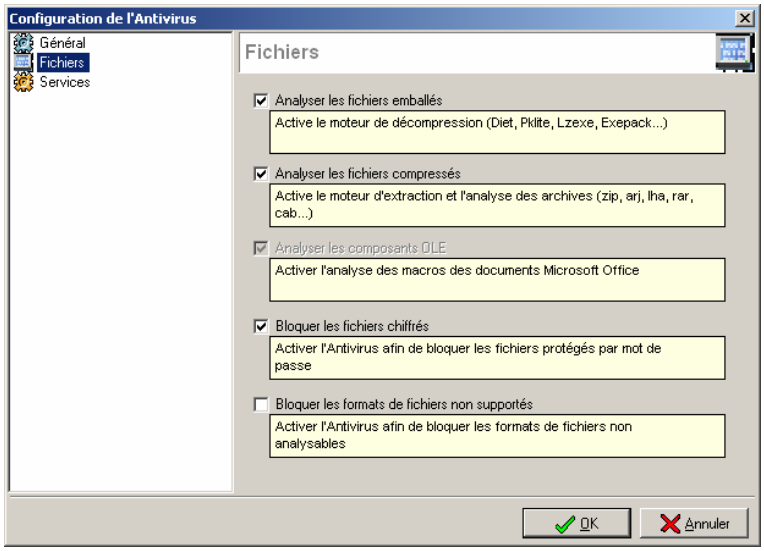


L'activation du service permet d'analyser les trafics SMTP, POP3 ou HTTP (suivant la configuration des proxies réalisée préalablement, voir Chapitre 5 Section A.

Le menu de configuration générale du service antivirus des IPS-Firewalls NETASQ est constitué de plusieurs options expliquées dans le tableau suivant :

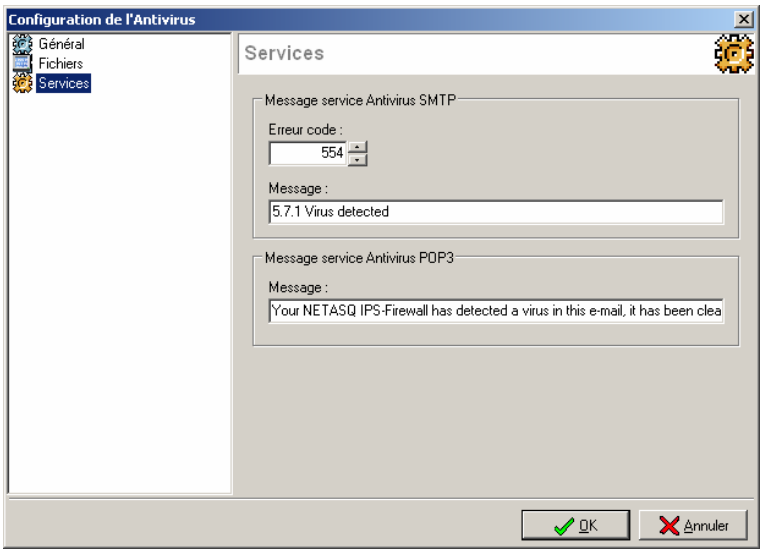
Activer le service Antivirus intégré	Cochez l'option pour activer la protection contre les virus. Par défaut l'antivirus ClamAV est utilisé pour fournir cette protection mais il est possible de bénéficier du service antivirus Kaspersky, pour cela contactez votre partenaire.
Version	Donnée informative indiquant la version du moteur antiviral intégrée dans ses produits IPS-Firewalls NETASQ.
Dernière mise à jour de la base antivirale	Donnée informative indiquant la date de la dernière mise à jour réussie de la base antivirale de l'antivirus. La mise à jour de la base antivirale est un élément important dans la garantie d'un service antivirus performant et efficace. En effet lorsqu'un nouveau virus apparaît, il est important de bénéficier au plus vite de sa signature pour s'en protéger. Les modalités de mise à jour automatique de la base antivirale sont définies dans l'Active Update.

Fichier


Configuration de l'Antivirus
Général
Fichiers
Services
Fichiers
Analyser les fichiers emballés
Active le moteur de décompression (Diet, Pklite, Lzexe, Exepack...)
Analyser les fichiers compressés
Active le moteur d'extraction et l'analyse des archives (zip, arj, lha, rar, cab...)
Analyser les composants OLE
Activer l'analyse des macros des documents Microsoft Office
Bloquer les fichiers chiffrés
Activer l'Antivirus afin de bloquer les fichiers protégés par mot de passe
Bloquer les formats de fichiers non supportés
Activer l'Antivirus afin de bloquer les formats de fichiers non analysables
OK
Annuler

Dans ce menu, vous configurez les types de fichiers qui doivent être analysés par le service Antivirus de l'IPS-Firewall NETASQ.

Services



La configuration avancée de l'antivirus Kaspersky intégré permet de personnaliser les réponses envoyées aux utilisateurs lorsqu'un mail contient un virus. Le tableau suivant explique les différents paramètres.

Code d'erreur	Code d'erreur SMTP renvoyé à l'expéditeur lors de la découverte d'un virus dans un trafic SMTP.
Message	Message associé au code d'erreur SMTP.
Message Antivirus pour le service POP3	Lors de la découverte d'un virus sur un trafic POP3, un email est créé par l'IPS-Firewall NETASQ. Il contient le message indiqué dans ce champ et une partie de l'email original (expéditeur,

	destinataire et sujet principalement). Cet email est alors envoyé par l'IPS-Firewall à l'émetteur de la requête POP3 sur laquelle a été découverte le virus.

Modification de l'antivirus du service antivirus

Lorsque le service antivirus en place ne convient plus à la structure du réseau, il est possible de remplacer ce service antivirus par l'autre offre de service proposée par NETASQ.

Ainsi si vous possédez l'antivirus ClamAV et que vous désirez vous procurer une offre de service maintes fois primée, tel que l'est l'antivirus Kaspersky, cela est possible.

Si vous possédez l'antivirus Kaspersky et que vous désirez vous procurer une offre de service gratuite, tel que l'est l'antivirus ClamAV, cela est possible. Et la méthode est la même.

Remplacer le service ClamAV par le service Antivirus Kaspersky

Pour modifier le service antivirus que vous possédez actuellement, reportez-vous à la procédure suivante :

1. Contactez votre partenaire pour souscrire au service antivirus Kaspersky, ce service est payant ;

2. Récupérez dans votre espace client, la licence de votre produit mis à jour (avec l'option Kaspersky activée) ;

3. Récupérez dans votre espace client, le package d'installation de l'antivirus Kaspersky (le package d'installation de l'antivirus Kaspersky se présente comme une mise à jour « classique » du firmware IPS-Firewall) ;

4. Insérez la nouvelle licence dans l'IPS-Firewall (l'insertion de cette licence ne désactive pas l'utilisation du service ClamAV) ;

5. Effectuez la mise à jour de l'IPS-Firewall avec le package d'installation de l'antivirus Kaspersky puis activez le nouveau service Antivirus.

Remplacer le service Kaspersky par le service Antivirus ClamAV

Pour modifier le service antivirus que vous possédez actuellement, reportez-vous à la procédure suivante :

1. Contactez votre partenaire pour souscrire au service antivirus ClamAV, ce service est gratuit mais il ne peut être obtenu qu'à la fin effective du service antivirus Kaspersky ;

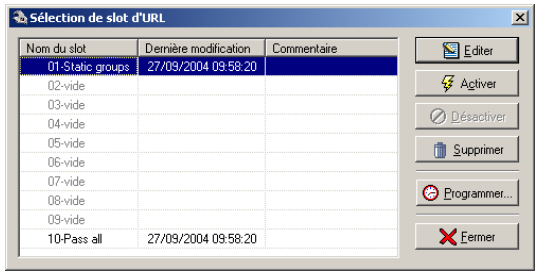
2. Récupérez dans votre espace client, la licence de votre produit mis à jour (avec l'option ClamAV activée) ;

3. Récupérez dans votre espace client, le package d'installation de l'antivirus ClamAV (le package d'installation de l'antivirus ClamAV se présente comme une mise à jour « classique » du firmware IPS-Firewall) ;

4. Insérez la nouvelle licence dans l'IPS-Firewall (l'insertion de cette licence ne désactive pas l'utilisation du service Kaspersky dans la durée de fonctionnement effectif du service souscrit) ;

5. Effectuez la mise à jour de l'IPS-Firewall avec le package d'installation de l'antivirus ClamAV puis activez le nouveau service Antivirus.

Lorsque vous sélectionner le sous menu « Analyse de contenu > Filtrage d'URLs > Règles de filtrage » une boîte de dialogue s'affiche, elle vous permet de manipuler les slots associés au filtrage URL.



Le filtrage URL est actif si un des fichiers de configuration est actif.

Elle est découpée en deux zones :

Gauche	Liste des slots.
Droite	Actions sur le slot sélectionné.

Liste des slots

Dans cette partie de la boite de dialogue se trouve la liste des slots. Il en existe 10, numérotés de 01 à 10.

Chaque slot possède un nom, une date/heure de mise en activité et la date de dernière modification effectuée sur ce slot. La programmation de l'activation de ces slots se fait grâce au programmateur horaire (Chapitre IV, Section D « programmation horaire »).

Le slot en cours d'activité est indiqué par une petite flèche verte à gauche de son nom. Un slot est dit "en activité" lorsque les paramètres qu'il contient sont en service. Il ne peut y avoir plus d'un slot en activité car les paramètres du dernier slot activé écrasent ceux du slot activé précédemment.

Si vous modifiez un slot, vous devez le réactiver pour prendre en compte les modifications. Un slot modifié mais non réactivé est notifié par l'icône à la place de la flèche verte habituelle.

Il est possible qu'il n'y ait aucun slot en activité, cela implique que tous les sites web sont bloqués (action par défaut) sauf si une règle autorisant le HTTP est ajoutée dans les règles de filtrage.

Chaque slot ne doit pas obligatoirement contenir des paramètres.

Un slot pour lequel il n'existe pas de fichier de configuration sur le Firewall NETASQ est affiché sous le nom « vide » dans la liste.

Un slot est dit sélectionné quand vous faites un simple clic de la souris sur son nom. La sélection faite, vous pouvez l'éditer ou l'activer.

© Copyright NETASQ 2006

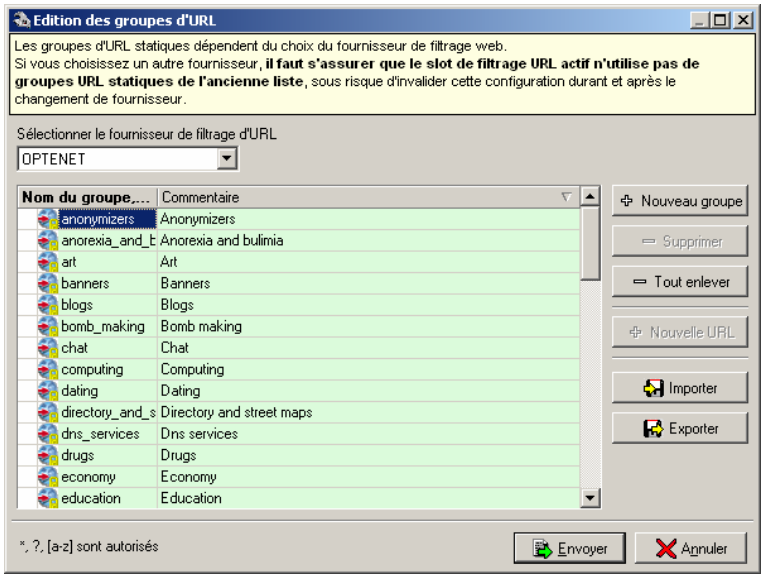
Actions sur le slot sélectionné

Quand un slot est sélectionné, vous pouvez réaliser différentes actions :

Editer	Modifier les règles de filtrage associées à ce slot.
Activer	Activer immédiatement un slot : les paramètres enregistrés dans ce slot écrasent les paramètres en vigueur. Lorsqu'on sélectionne un slot déjà activé ce bouton se transforme en un bouton « désactiver » pour réaliser l'action de désactivation.
Programmer	Donner l'heure et le ou les jours auxquels le fichier va s'activer automatiquement.
Effacer	Effacer le slot et toutes ses informations.
Fermer	Retour à l'écran principal.

Par défaut un slot de filtrage d'URL a été configuré. Ce slot n'est pas actif mais peut l'être. Il est un exemple des possibilités offertes par le filtrage d'URL NETASQ.

La création de groupes d'URLs va accélérer la saisie des règles de filtrage. Chaque groupe contient une liste de masques d'URLs et permet par exemple de représenter les besoins de chaque service au sein d'une entreprise. La création des groupes d'URL est accessible via le menu « Analyse de contenu > Filtrage d'URLs > Groupes d'URLs ».



Vous pouvez, au niveau de la configuration des groupes, effectuer les actions suivantes :

Nouveau groupe	Crée un nouveau groupe.
Supprimer	Supprime un groupe ou une URL existant. Sélectionnez la ligne à supprimer puis cliquez sur ce bouton.
Nouvelle URL	Ajoute une URL à un groupe. Sélectionnez d'abord le groupe dans lequel vous voulez ajouter une URL puis cliquez sur ce bouton.
Importer	Permet d'importer une liste d'URLs contenue dans un fichier .txt. Vous devez d'abord créer un nouveau groupe et lui affecter un nom. Cliquez ensuite sur le bouton "Importer" et choisissez le fichier concerné. Les URLs contenues dans le fichier seront alors intégrées au groupe. **Si ce groupe contenait déjà des URLs, celles-ci seront écrasées.**
Exporter	Permet d'exporter une liste d'URLs contenue dans un groupe. Choisissez le groupe dont vous voulez exporter la liste, puis cliquez sur le bouton "Exporter". La liste sera enregistrée dans un fichier texte.
Le fournisseur de filtrage d'URL	Il existe deux types de groupes d'URL : des groupes d'URL statiques (entrés manuellement par l'administrateur) et des groupes d'URL dynamiques (Voir la section « Filtrage d'URL dynamique » ci-dessous). Le fournisseur demandé est le fournisseur des groupes d'URL dynamiques, par défaut « NETASQ ».

© Copyright NETASQ 2006

Format du fichier d'URLs

Les fichiers texte pour l'import ou l'export d'URLs doivent être formatés de la façon suivante :

URL1
URL2
URL3
...

Vous pouvez éditer vos listes dans un éditeur de texte et les importer ensuite au niveau du firewall.

La saisie d'un masque d'URL peut comporter la syntaxe suivante :

*****	Remplace une séquence de caractères quelconque. Par exemple, *.netasq.com/permet de définir le domaine Internet de la société NETASQ.
?	Remplace un caractère. Par exemple ???.netasq.com est équivalent à www.netasq.com ou de ftp.netasq.com mais pas à www1.netasq.com.
[a-z]	Remplace un intervalle de caractère. Par exemple ftp[1-2].netasq.com est équivalent à ftp1.netasq.com et à ftp2.netasq.com.

Un masque d'URL peut contenir une URL complète (exemple : www.netasq.com*) ou des mots-clés contenus dans l'URL (exemple : *mail*).

Il est aussi possible de filtrer des extensions de fichiers :

Exemple : le masque d'URL '*.exe' peut servir à filtrer les fichiers exécutables.

Vous pouvez afficher ou masquer le contenu de chaque groupe d'URLs en cliquant sur les icônes "+" ou "-".

Filtrage d'URL dynamique

Le filtrage d'URL dynamique disponible sur les appliances NETASQ vous permet de réaliser du filtrage d'URL au moyen de listes d'URL renseignées et actualisées dynamiquement grâce à la fonctionnalité « d'Active Update » (Voir « Configuration Active Update »).

Ces URL sont classées par catégories. Chacune des catégories contient une liste d'URL répertoriées que vous pouvez autoriser ou interdire.

Il est impossible de visualiser les URL contenues dans ces groupes car ils sont compressés et optimisés pour leur traitement par l'IPS-Firewall, elles ne sont donc pas modifiables. Un cadenas jaune apparaît sur les groupes d'URL dynamique.

Fournisseur des listes d'URL

Suivant le type de service de maintenance souscrit (Voir la politique tarifaire NETASQ en cours), les listes d'URLs disponibles sont mises à jour dynamiquement par des fournisseurs différents (parmi NETASQ ou OPTENET). Aujourd'hui, NETASQ a catégorisé deux types de fournisseurs : NETASQ

en lui-même et OPTENET. Par défaut lorsqu'un service de maintenance « standard » est souscrit, ce sont les listes d'URL NETASQ qui sont proposées.

Lorsque vous souscrirez au service de maintenance incluant OPTENET, pour activer la fonctionnalité de filtrage d'URL sur les listes d'URL OPTENET, sélectionnez dans la liste des fournisseurs proposés : OPTENET. A la fermeture du menu des groupes d'URL, l'appliance prendra en compte la demande et effectuera le téléchargement des nouvelles listes d'URL grâce au module Active Update.

Lorsque vous modifiez le fournisseur des groupes d'URL, assurez-vous que le slot de filtrage d'URL actif ne sera pas affecté par la perte des anciens groupes d'URL. Si le slot actif est impacté, désactivez le.

Requête d'ajout d'URL

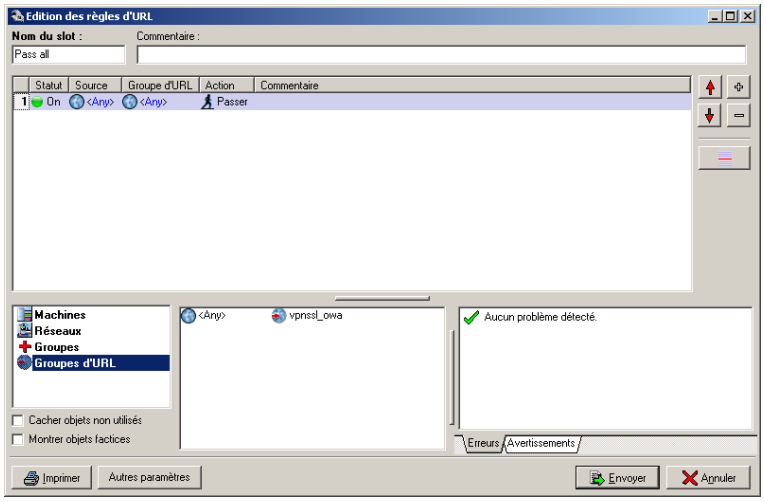
NETASQ a mis en place sur son site WEB, un formulaire vous permettant de demander l'ajout d'une URL qui serait inconnue dans les groupes d'URL dynamique. Ce formulaire est disponible à l'adresse suivante : http://www.netasq.com/updates/urlfiltering.php. NETASQ se réserve le droit de ne pas donner suite à cette requête (pour une raison de validité de la demande, l'adresse ne correspond à aucune catégorie déjà définie…).

Notez qu'il est toujours possible de rajouter manuellement cette adresse dans un groupe d'URL « statique » et de l'ajouter au filtrage.

Reportez-vous à la procédure suivante pour éditer un slot de filtrage d'URL :

1. Sélectionnez un slot dans la liste des slots de filtrage d'URL,

2. Cliquez sur le bouton « Editer » de la boite de dialogue contenant la liste des slots de filtrage d'URL.



La fenêtre d'édition d'un slot de filtrage d'URL apparaît. Elle est composée de plusieurs parties :

- ► Une grille contenant les règles de filtrage ;
- ► Un menu Drag'n Drop ;
- ► Un analyseur de cohérence et de conformité des règles ;
- ► Une zone d'actions possibles.

Règles de filtrage

Cette zone de la boîte de dialogue contient une grille vous permettant de définir les règles de filtrage URL à appliquer. Pour éditer les règles, il suffit de double cliquer sur la zone à modifier.

Statut	Etat de la règle : ON, la règle sera active lorsque ce slot de filtrage sera actif. OFF, la règle ne sera pas active lorsque ce slot sera actif.
Action	Permet de spécifier le résultat de la règle, **passer** pour autoriser le site, **bloquer** pour interdire l'accès sans message de blocage, **page blocage** pour interdire l'accès et afficher la page de blocage.
Source	A quel utilisateur, machine, groupe de machines ou réseau s'applique la règle.
Groupe	Un nom de groupe d'URL précédemment créé. En double-cliquant sur le champ, une boîte de dialogue vous invite à choisir un groupe d'URLs. Le groupe <Any> correspond à toutes les URLs.

© Copyright NETASQ 2006

Commentaire	Commentaire associé à la règle.

Au niveau de la source, vous pouvez définir les utilisateurs ou groupes d'utilisateurs qui doivent s'authentifier pour accéder à certains sites (vous pouvez autoriser certains sites uniquement pour certains utilisateurs). L'utilisateur devant s'authentifier verra une page d'authentification apparaître dans son navigateur lorsqu'il essaiera de se connecter à un site WEB.

A la gauche des noms d'objets se trouve un voyant d'état :

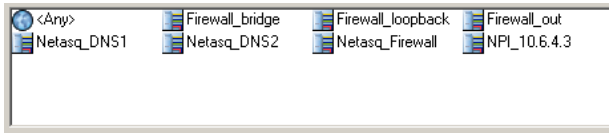
- La règle est appliquée,
- La règle est ignorée.

Le Firewall va évaluer les règles une à une en partant du haut. Dés qu'il rencontre une règle qui correspond à la demande il effectue l'action spécifiée et ne descend plus dans les règles. Si aucune règle n'est valable, le Firewall utilisera le paramétrage par défaut. (autorisation ou blocage selon la sélection ou non de l'option "Autoriser l'accès si aucune règle ne correspond" présente dans la fenêtre "Autres paramètres").

Actions possibles

Nom du slot	Nom donné au fichier de configuration.
Commentaire	Commentaire indicatif associé au slot de filtrage
Insérer	Insérer une ligne vierge après la ligne sélectionnée.
Effacer	Supprimer la ligne sélectionnée.
Flèche vers le haut	Placer la ligne sélectionnée avant la ligne directement au dessus.
Flèche vers le bas	Placer la ligne sélectionnée après la ligne directement en dessous.
Insérer un séparateur	Cette option permet d'insérer un séparateur au dessus de la ligne sélectionnée afin d'indiquer un commentaire sur une ligne de l'édition du filtrage. Pour définir un séparateur, il s'agit d'indiquer un commentaire et une couleur pour ce séparateur.
Imprimer	Impression de la configuration du filtrage d'URL.
Autres Paramètres	Permet de spécifier le fonctionnement du filtrage d'URL. Cochez l'option « Autoriser l'accès si aucune règle ne correspond » pour un fonctionnement de type « Liste noire d'URL ».

Menu Drag & Drop



© Copyright NETASQ 2006

Comme son nom l'indique le menu « Drag'n Drop » permet en un Drag & Drop de positionner les objets configurés dans le chapitre précédent dans les règles de filtrage. L'opération de Drag & Drop consiste à :

- ► Sélectionner un objet,
- ► Maintenir le bouton de souris enfoncé,
- ► Réaliser un glissement de l'objet vers la grille de règles,
- ► Enfin y déposer l'objet.

Lorsque l'administrateur réalise une opération de Drag'n Drop, les champs disponibles pour l'objet sélectionné apparaissent en surbrillance.

Le menu de sélection des types d'objet situé à gauche du menu Drag'n Drop permet de sélectionner le type d'objet affiché dans la grille.

Affichage de la grille

L'affichage des données contenues dans la grille peut être défini suivant les préférences de l'administrateur parmi les options d'affichage : grandes icônes, petites icônes, détaillé ou en liste.

Options d'affichage

Deux options d'affichage des données de la grille du menu Drag'n Drop sont disponibles.

Montrer que les objets utilisés

Comme son nom l'indique, cette option permet d'afficher dans la grille que les objets qui sont actuellement utilisés dans les règles de translation.

Montrer les objets spéciaux

Les objets spéciaux sont les objets créés par défaut par l'IPS-Firewall et qui seront utilisés à l'activation des services associés (par exemple : Firewall_pptpXX, Firewall_dialupXX, Firewall_ipsec…). Ces objets rendent la lecture générale difficile et sont cachés par défaut.

Analyseur de cohérence et de conformité des règles

De la même façon que pour l'édition des règles de filtrage et de translation, l'écran d'édition des règles de filtrage d'URLs des IPS-Firewalls dispose d'un analyseur de cohérence et de conformité des règles qui prévient l'administrateur en cas d'inhibition d'une règle par une autre ou d'erreur sur une des règles qui a été créées.

Divisé en deux onglets, cet analyseur regroupe les erreurs de création de règles dans l'onglet « Erreurs » et les erreurs de cohérence dans les règles dans l'onglet « Avertissements ».

Envoi des modifications au Firewall NETASQ

Cliquez sur le bouton « Envoyer » pour stocker le fichier sous le nom défini dans la zone de saisie « Nom ».

Lors de l'envoi du slot à l'IPS-Firewall NETASQ, le logiciel de configuration vérifie le nom que vous avez attribué au slot. En aucun cas le nom de fichier ne peut valoir « vide » ou avoir pour valeur un nom de slot existant. Si tel est le cas, le logiciel affiche une boîte de dialogue vous invitant à modifier le nom du slot (« Nom »).

Après avoir cliqué OK, vous êtes libre de modifier le champ « Nom », ainsi que tous les autres paramètres.

La modification d'un slot de filtrage URL n'est pas dynamique. Les modifications ne seront effectives qu'à la prochaine activation du slot sur le Firewall NETASQ.

Modules de filtrage URL complémentaires

X-Stop

Pour installer le module de filtrage X-Stop, reportez-vous à la procédure suivante :

1. Installez le logiciel 'X-Stop for NT server' sur un serveur,

2. Configurez les champs « Activer le filtrage par serveur X-Stop » dans la configuration du proxy HTTP (Voir la « configuration du proxy HTTP ») avec l'adresse et le port du serveur X-Stop (13111 par défaut),

Pour plus d'information sur l'utilisation de l'interface graphique X-Stop vous pouvez consulter la notice du logiciel.

Websense

Un IPS-Firewall avec la fonction « Activer la redirection vers un autre serveur proxy » permet de faciliter la mise en place d'un serveur Websense. Pour installer le module de filtrage Websense, reportez-vous à la procédure suivante :

1. Installez 'Websense for proxy server' sur un serveur,

2. Configurez les champs "Activer la redirection vers un autre serveur proxy" dans la configuration du proxy HTTP (Voir la « configuration du proxy HTTP ») avec l'adresse et le port du serveur Websense.

Section C

Services

Introduction

La gestion du réseau est assurée par des applications qui monitorent et contrôlent l'état des différents éléments d'un réseau. Ces éléments peuvent être des stations de travail, des serveurs, des passerelles qui contiennent les agents de gestion requis par ces applications de gestion du réseau. Les agents remontent des informations de gestion qui sont exploitées par les applications. Le SNMP est utilisé pour la communication entre les agents et les applications.

SNMP utilise le protocole UDP par conséquent les paquets échangés entre la station de gestion (client) et l'agent (serveur) présent sur l'élément de réseau sont des datagrammes sans garantie d'arrivée.

Il existe deux types d'échanges entre le client et le serveur :

► soit le client envoie une requête et le serveur répond,
► soit c'est le serveur qui prend l'initiative en envoyant une alarme (traps) à la station de gestion pour lui indiquer qu'un événement important est survenu.

L'agent (serveur) écoute sur le port UDP 161 et la station de gestion écoute les traps (alarmes) sur le port 162.

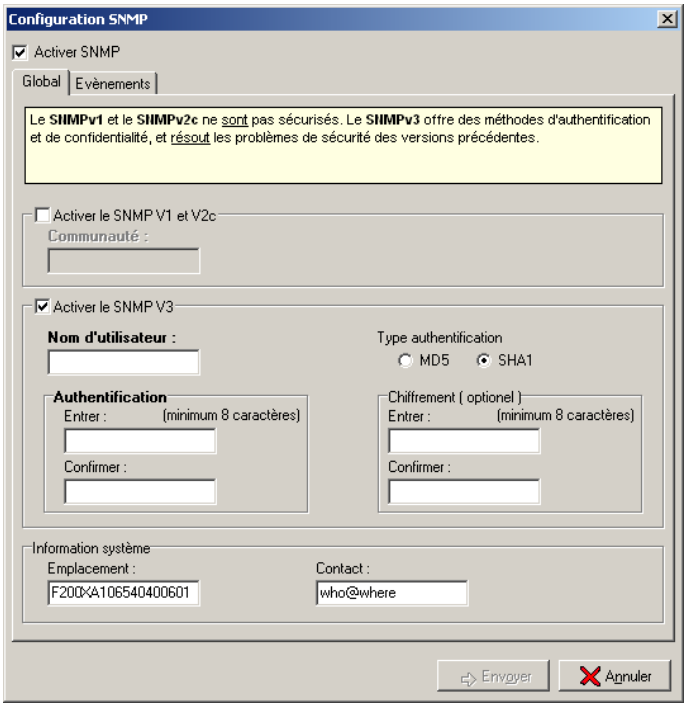
Utilisation du service SNMP du firewall NETASQ

Le service SNMP du firewall NETASQ est un serveur qui peut vous permettre de monitorer l'état du firewall. Le firewall peut donc être intégré dans une solution de gestion de réseau tel Tivoli ou HP OpenView.

Fonctionnement

Pour utiliser le service SNMP, celui-ci doit être activé. L'activation du service est réalisée au niveau du menu « Services > SNMP ».

© Copyright NETASQ 2006



L'écran de configuration du service SNMP se décompose en deux parties :

► L'onglet Global : cet écran vous permet de spécifier la version du protocole SNMP utilisé et les informations relatives à chaque version,

► L'onglet Evénements : dans cet onglet vous spécifiez vers quels hôtes doivent être envoyés les informations remontées par le firewall.

Global

Le protocole SNMP fonctionne selon ce qu'on pourrait appeler deux « modes ». Soit une station de gestion vient chercher les informations auprès de l'élément du réseau, soit c'est l'élément de réseau qui remonte ces informations de gestion auprès d'une station qui lui est spécifiée.

Dans cet onglet, vous configurez les informations nécessaires à l'établissement d'une connexion entre le firewall et la station de gestion lorsque celle-ci cherche à obtenir des données de gestion.

SNMP V1 et V2c

Les premières versions du protocole SNMP ne sont pas très sécurisées. Le seul champ nécessaire est le nom de la communauté. Par défaut la RFC propose le nom « public ».

Nous vous conseillons toutefois de ne pas l'utiliser pour des raisons de sécurité.

SNMP V3

Depuis décembre 2002, un nouveau standard existe pour le protocole SNMP, il apporte une avancée significative en matière de sécurité. La configuration requiert les paramètres suivants :

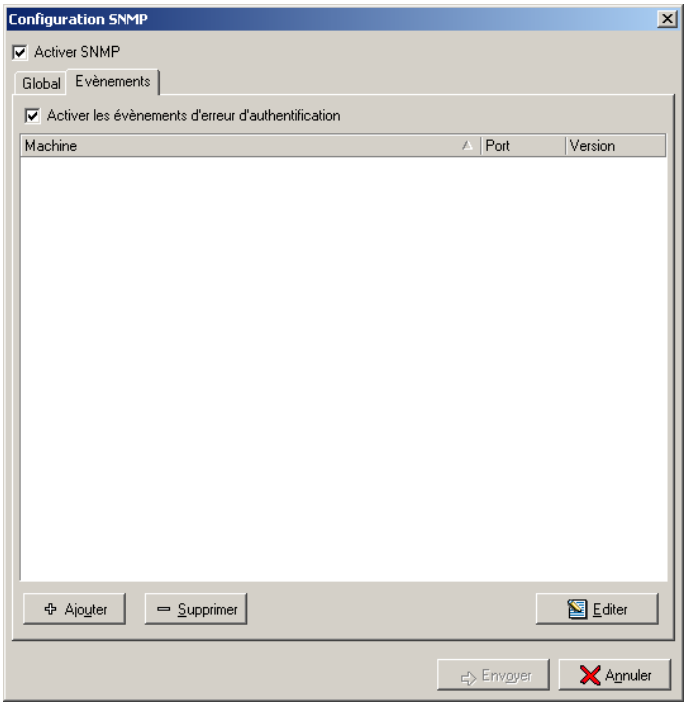
Nom d'utilisateur	Nom d'utilisateur utilisé pour la connexion.
Type Authentification	Deux types d'authentification sont disponibles, le MD5 et le SHA1.

Authentication	Mot de passe de l'utilisateur.
Chiffrement	Les paquets SNMP sont chiffrés en DES, une clef de chiffrement peut être définie. Par défaut c'est la clef d'authentification qui est utilisée. **Il est vivement recommandé d'utiliser une clef spécifique**.

Information système

Emplacement	Information de lieu sur l'élément surveillé.
Contact	Adresse mail de la personne à contacter en cas de problème.

Evénements



Dans cet onglet, vous configurez les stations que doit contacter l'IPS-Firewall lorsqu'il veut envoyer une Trap SNMP (événement). Si aucune station (hôte) n'est spécifiée, l'IPS-Firewall n'envoie pas de messages.

En activant l'option « Activer les événements d'erreur d'authentification » vous pourrez recevoir les informations concernant les erreurs de connexion.

Un assistant vous guide dans la configuration des hôtes.

La configuration d'un hôte dans l'assistant se déroule comme pour l'onglet global. La sélection d'une version du protocole SNMP détermine le type de configuration à effectuer.

SNMP V1 et V2c

Dans ce cas, seul un nom de communauté est nécessaire.

SNMP V3

Les paramètres de la configuration des évenements de type SNMP V3 sont les suivants :

Authentication	Deux types d'authentification sont disponibles, le MD5 et le SHA1.
Security name	Nom de l'utilisateur autorisé à envoyer une trap sur la station de gestion.
Engine ID	chaîne en hexadécimal créé par la station de gestion pour identifier l'utilisateur de manière unique.
Niveau de sécurité	Différents niveaux de sécurité sont disponibles pour la version du protocole SNMP : ► Pas d'authentification et de chiffrement : aucune sécurité, ► Authentification et pas de chiffrement : authentification sans chiffrement des traps, ► Authentification et chiffrement. Si le mot de passe chiffrement reste vide on utilise le mot de passe authentification pour le chiffrement.
Mot de passe authentification	Mot de passe de l'utilisateur.
Mot de passe chiffrement	Les paquets SNMP sont chiffrés en DES, une clef de chiffrement peut être définie. Par défaut c'est la clef d'authentification qui est utilisée. **Il est vivement recommandé d'utiliser une clef spécifique.**

Le bouton d'action « Editer » permet de modifier les informations concernant un hôte une fois que celui-ci a été créé.

Introduction

Le DHCP fournit des paramètres de configuration pour des machines Internet. Il est constitué de 2 parties : Un protocole pour la livraison de paramètres de configuration de machines spécifiques à partir d'un serveur DHCP et un mécanisme d'allocation d'adresses réseau à des machines.

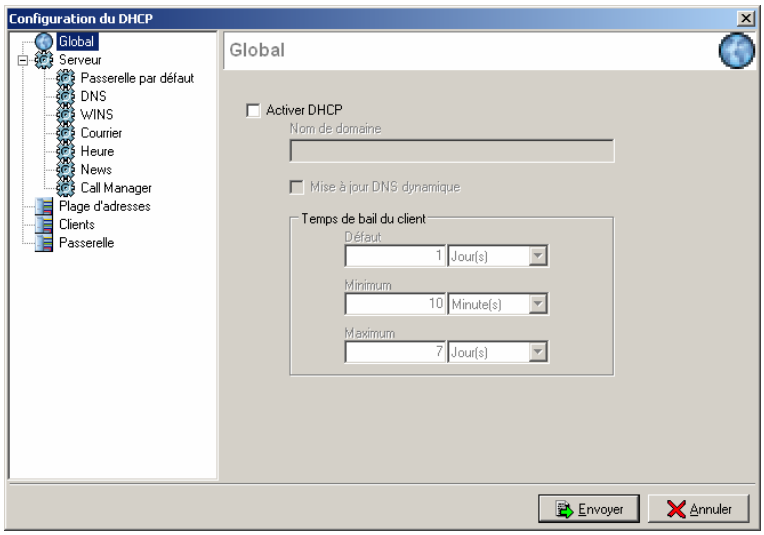
DHCP est bâti sur le modèle client - serveur. Le terme "serveur" se réfère à une machine fournissant des paramètres d'initialisation au travers du DHCP, et le terme "client" se réfère à une machine qui utilise DHCP pour obtenir des paramètres de configuration telle qu'une adresse réseau.

Utilisation du service DHCP du firewall NETASQ

Le service DHCP de NETASQ est un serveur qui peut vous permettre d'allouer des adresses réseau et de délivrer des paramètres de configuration à des machines configurées dynamiquement.

Fonctionnement

Pour utiliser le service DHCP, celui-ci doit être activé. L'activation du service est réalisée au niveau du menu « Services > DHCP ».



L'écran de configuration du service DHCP se décompose en deux parties :

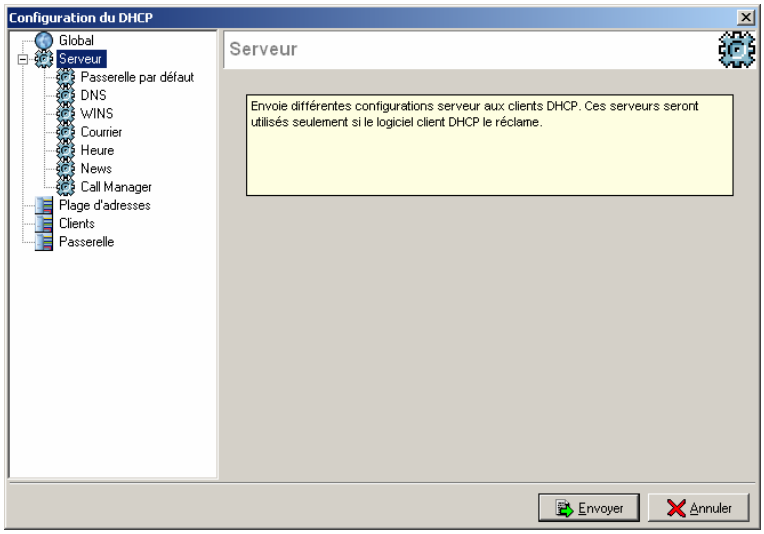
► A gauche un arbre présentant les diverses fonctionnalités du menu Service DHCP,
► A droite les options configurables.

© Copyright NETASQ 2006

Global

Nom de domaine	Nom de domaine utilisé pour la définition des utilisateurs.
Mise à jour DNS dynamique	Mise à jour dynamique du DNS. Lorsque les informations contenues par le serveur DHCP sont modifiées, le serveur DNS 1 (configuré dans le menu serveur DNS) est dynamiquement mis à jour).
Temps de bail du client	Temps pendant lequel les stations garderont la même adresse IP. Une valeur par défaut, au minimum et au maximum.

Serveur



Ce menu est réservé à la configuration des adresses des différents serveurs : passerelle par défaut, DNS, WINS, Courrier (SMTP et POP), Heure (NTP), News (NNTP) et Call Manager (MGCP). Ces adresses seront automatiquement envoyées aux stations pour qu'elles puissent contacter les serveurs correspondants.

Deux modes d'attribution sont possibles :

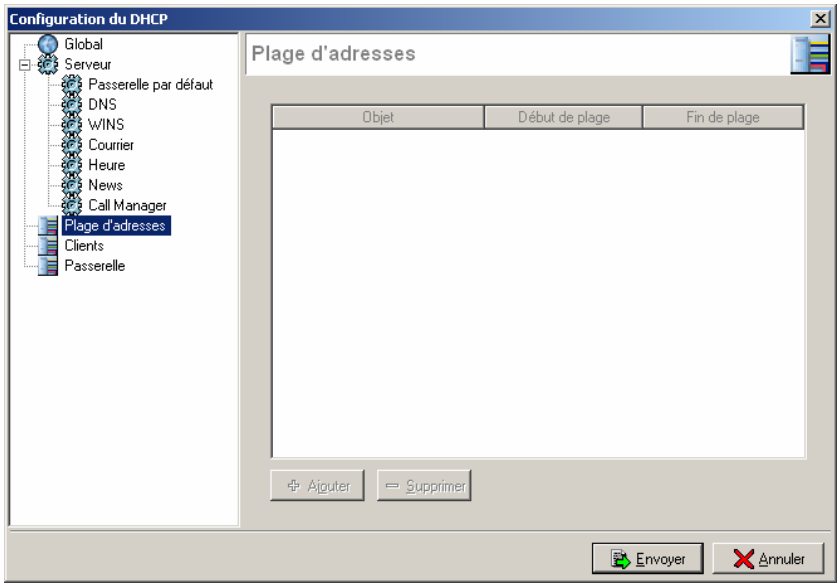
- ► par plage,
- ► par hôte.

Par plage vous spécifiez un groupe d'adresses destinées à être allouée aux utilisateurs. L'adresse allouée l'est alors pour temps déterminé dans la configuration globale. Dans la configuration DHCP par hôte, l'adresse allouée par le service est toujours la même : celle indiquée dans le menu « hôte ». Il s'agit en réalité d'un adressage « statique » mais qui permet de « libérer » le poste client de sa configuration réseau.

Rappel pour les Serveurs DNS

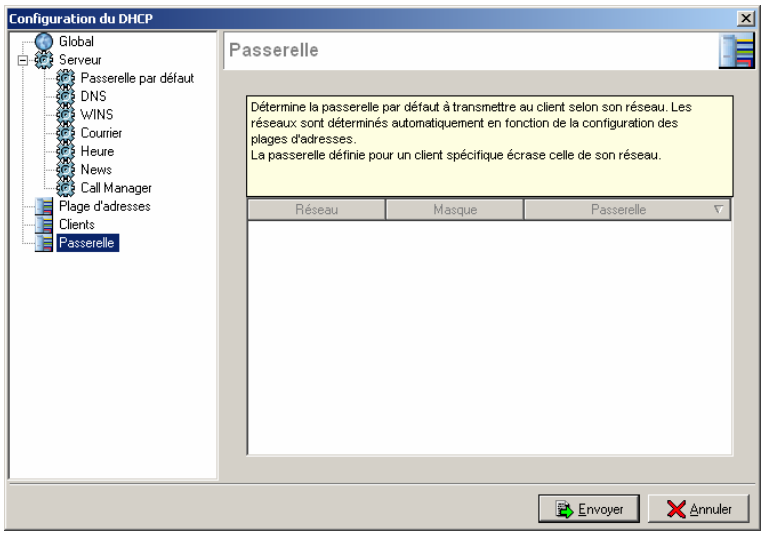
Si l'IPS-Firewall obtient l'adresse IP d'une des interfaces par DHCP et que l'option « Requêtes DNS » est configurée, alors il est possible de définir dans la configuration du service DHCP, les serveurs DNS obtenus par l'IPS-Firewall auprès du fournisseur d'accès. Ces serveurs sont identifiés dans la configuration des objets par les machines « Firewall_<nom de l'interface>_dns1 » et « Firewall_<nom de l'interface>_dns2 ».

Plage d’adresses



Ce menu vous permet de spécifier les plages d’adresses IP qui seront automatiquement attribuées et les passerelles par défaut associées. En ajoutant une plage d’adresse IP, le firewall détermine automatiquement l’adresse réseau et la passerelle associée à ce réseau.

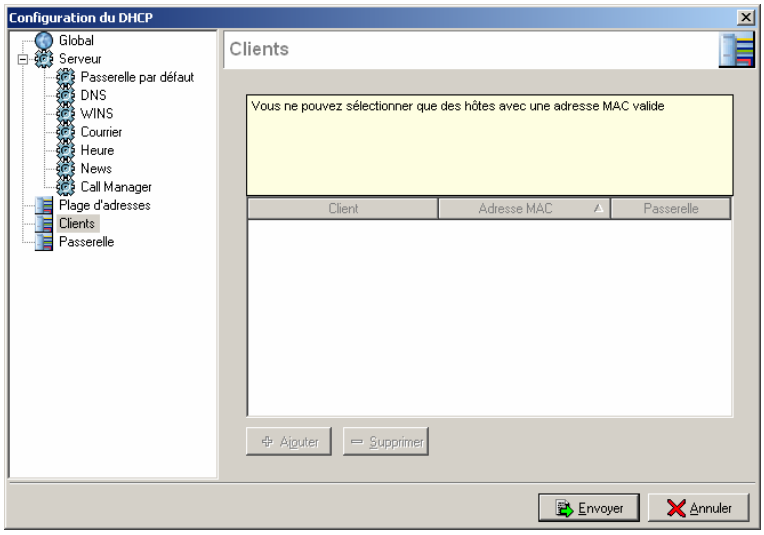
Lors de l’ajout d’une passerelle, le firewall manager ne propose que les objets associés au réseau.



Attention deux plages ne peuvent se chevaucher. Une plage d’adresses appartient à un unique bridge/interface. Un hôte ne peut être défini dans une plage. La passerelle définie pour un réseau appartient à ce réseau.

Seul les objets de type « plage d’adresses » sont autorisés dans cette configuration.

Clients



Dans le menu « Clients », il est possible de définir une adresse IP et une passerelle par défaut spécifique pour un poste client possédant une adresse MAC donnée. Cette configuration se rapproche d'un adressage statique mais rien n'est indiqué sur le poste client ainsi la gestion des adresses allouées et de la configuration des postes clients est simplifiée.

© Copyright NETASQ 2006

Introduction

L'objectif de cette introduction n'est pas d'expliquer ce qu'est un DNS. Pour obtenir de plus amples informations à ce sujet, il suffit de consulter un ouvrage générique sur les réseaux.

Ici nous voulons rappeler une partie du fonctionnement du DNS.

Le fonctionnement du DNS est de type client-serveur. La partie client s'appelle le *resolver*, c'est une bibliothèque. La partie serveur s'appelle le *name server*.

Il existe trois types de name server :

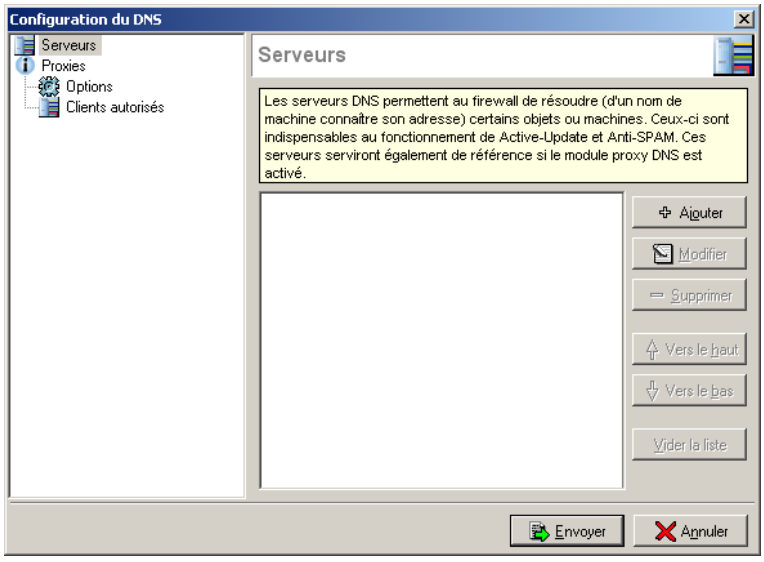
- primaire, possède les tables à jour d'un domaine,
- secondaire, possède les tables à jour provenant d'un autre serveur,
- cache, possède des tables construites à partir des informations traitées.

Utilisation possible du service DNS du firewall NETASQ

Le service DNS de NETASQ est un cache. Lorsqu'une requête DNS est envoyée au travers du firewall, celui-ci garde en mémoire (dans le cache DNS) la réponse et cela pour garantir un meilleur temps de réponse lors d'une prochaine requête DNS similaire. De plus, le firewall intercepte et reçoit la requête assurant ainsi un niveau de sécurité optimum.

Fonctionnement

Pour utiliser le service DNS, celui-ci doit être activé. L'activation du service est réalisée au niveau du menu « Services > DNS ».


Configuration du DNS
Serveurs
Proxies
Options
Clients autorisés
Serveurs
Les serveurs DNS permettent au firewall de résoudre (d'un nom de machine connaître son adresse) certains objets ou machines. Ceux-ci sont indispensables au fonctionnement de Active-Update et Anti-SPAM. Ces serveurs serviront également de référence si le module proxy DNS est activé.
Ajouter
Modifier
Supprimer
Vers le haut
Vers le bas
Vider la liste
Envoyer
Annuler

L'écran de configuration du service DHCP se décompose en deux parties :

► A gauche un arbre présentant les diverses fonctionnalités du menu Service DNS,
► A droite les options configurables.

Le service DNS proposé par l'IPS-Firewall NETASQ est un cache DNS. Celui-ci vise à garder en mémoire des réponses DNS contenant les correspondances entre noms de domaine et adresses IP.

Serveurs

Les serveurs permettent à l'IPS-Firewall de résoudre (connaître l'adresse IP d'une machine à partir de son nom) certains objets ou machines. Ceux-ci sont indispensables au fonctionnement de l'Active Update et l'Antispam. Ces serveurs serviront également de référence si le proxy DNS est activé.
Lorsque des serveurs sont configurés, les modules d'Antispam, d'Antivirus et de résolution des objets effectuent leur requête vers ces serveurs sans que le proxy DNS de l'IPS-Firewall (cache DNS) soit nécessairement activé. Dans ce cas, si un utilisateur envoie une requête DNS sur un serveur non configuré, la requête est transmise par l'IPS-Firewall au dit serveur et un utilisateur envoyant une requête DNS à l'IPS-Firewall voit sa requête refusée.

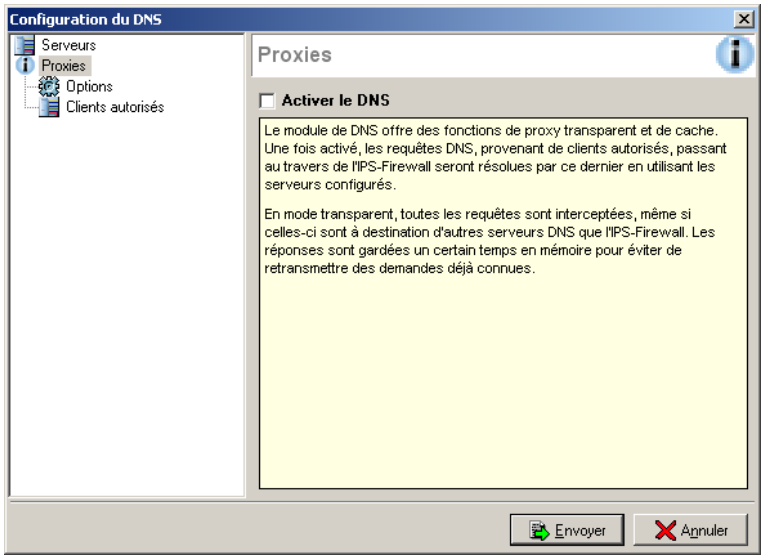
Si le proxy DNS (cache DNS) est activé (Voir activation du cache DNS ci-dessous), les modules d'Antispam, d'Antivirus et de résolution des objets effectuent leur requête vers les serveurs configurés sans toutefois faire appel au cache DNS. Si un utilisateur envoie une requête DNS sur un serveur non configuré, la requête est transmise par l'IPS-Firewall au dit serveur. Et lorsqu'un utilisateur envoie une requête DNS à l'IPS-Firewall, sa requête est alors traitée par le cache DNS.

Enfin si le proxy DNS est activé et le mode transparent configuré (Voir la configuration du mode transparent ci-dessous), les modules d'Antispam, d'Antivirus et de résolution des objets effectuent leur requête vers les serveurs configurés en utilisant le cache DNS. Si un utilisateur envoie une requête DNS sur un serveur non configuré, la requête est redirigée de manière transparente par l'IPS-Firewall vers les serveurs configurés dans ce module. Et lorsqu'un utilisateur envoie une requête DNS à l'IPS-Firewall, sa requête est alors traitée par le cache DNS.

Barre d'action

Ajouter	Ajout d'un serveur DNS.
Modifier	Modifier le serveur DNS sélectionné.
Supprimer	Supprimer le serveur DNS sélectionné.
Vers le haut	Placer la ligne sélectionnée avant la ligne directement au dessus.
Vers le bas	Placer la ligne sélectionnée après la ligne directement en dessous.
Vider la liste	Suppression de la liste complète des serveurs.

Proxies


Configuration du DNS
Serveurs
Proxies
Options
Clients autorisés
Proxies
Activer le DNS
Le module de DNS offre des fonctions de proxy transparent et de cache. Une fois activé, les requêtes DNS, provenant de clients autorisés, passant au travers de l'IPS-Firewall seront résolues par ce dernier en utilisant les serveurs configurés.
En mode transparent, toutes les requêtes sont interceptées, même si celles-ci sont à destination d'autres serveurs DNS que l'IPS-Firewall. Les réponses sont gardées un certain temps en mémoire pour éviter de retransmettre des demandes déjà connues.
Envoyer
Annuler

Mode transparent	Comme son nom l'indique cette option vise à rendre transparent le service DNS du firewall NETASQ. Ainsi lorsque cette option est activée la redirection des flux DNS vers le cache DNS est invisible aux utilisateurs qui pensent accéder à leur serveur DNS.
Taille du cache	Taille allouée au cache DNS.
Liste des clients autorisés	Liste des clients autorisés à émettre une requête DNS. Cette liste peut contenir des réseaux.

Introduction

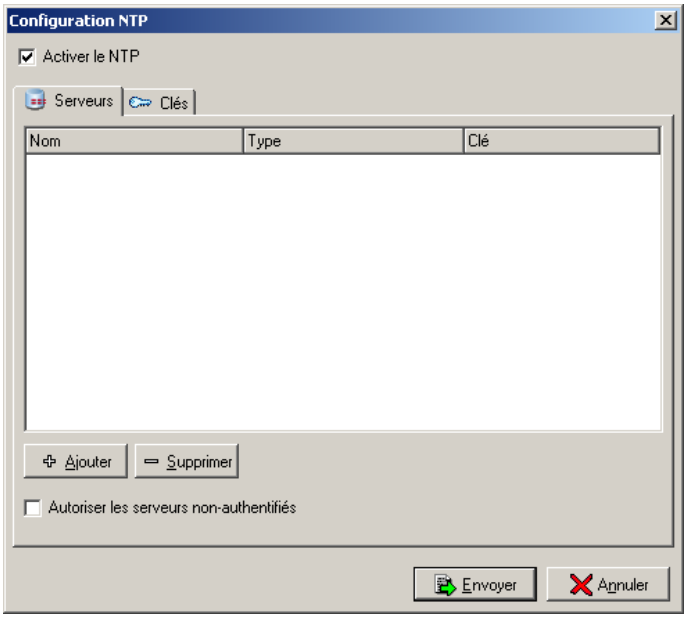
Ce protocole permet la synchronisation des horloges réseau de clients et serveurs répartis. NTP est construit sur le protocole UDP ce qui en fait un protocole du type non connecté. C'est en réalité une version évoluée des mécanismes Time Protocol et ICMP Timestamp message et un remplaçant tout à fait approprié. NTP fournit des mécanismes de synchronisation du temps avec une précision de l'ordre de la nanoseconde, tout en préservant une date non-ambiguë. Ce protocole inclut la possibilité de spécifier des informations sur la précision et l'erreur estimée de l'horloge locale ainsi que des indications sur l'horloge de référence auprès de laquelle elle peut se synchroniser.

Utilisation possible du service NTP du firewall NETASQ

Le protocole NTP se base sur une structure arborescente dans laquelle l'IPS-Firewall n'est qu'un client.

Fonctionnement

Pour utiliser le service NTP, celui-ci doit être activé. L'activation du service est réalisée au niveau du menu « Services > NTP ».



L'écran de configuration du service NTP se décompose en deux parties :

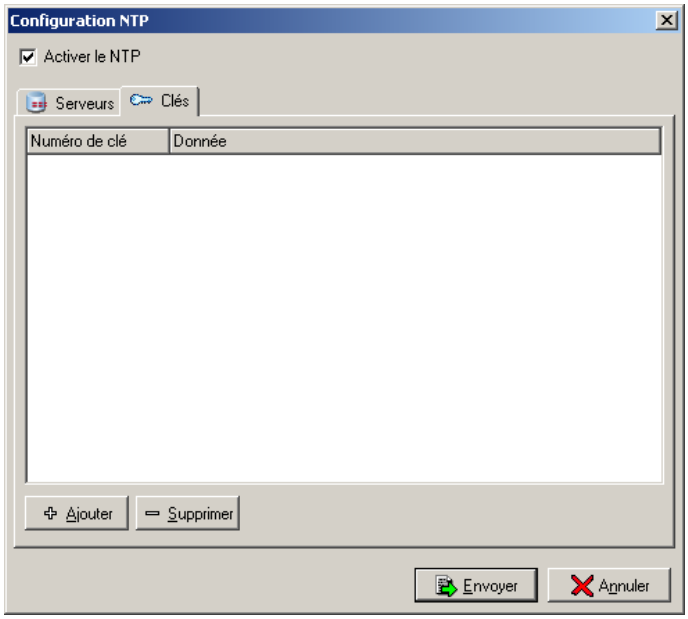
- L'onglet Serveurs : liste des serveurs NTP publics ou privés,
- L'onglet Clés : liste des clefs d'authentification.

© Copyright NETASQ 2006

Serveurs

Serveurs	Liste des serveurs NTP publics ou privés auxquels l'IPS-Firewallpourra se connecter pour se synchroniser.
Autoriser les serveurs non-authentifiés	Cette option vous permet d'autoriser l'utilisation de serveurs ne demandant aucune authentification.

Clés



Cet onglet vous permet de configurer des clefs pour l'authentification auprès de serveurs NTP. Cette clef est apparente si vous vous connectez avec les droits de modifications. Sinon elle est cachée.

Chapitre VII

Configuration de l'authentification

© Copyright NETASQ 2006

Les fonctions d'identification / authentification permettent à l'utilisateur de déclarer son login (identification) et de vérifier que cet utilisateur est bien la personne qu'il prétend être, par la fourniture d'éléments qu'il est censé être le seul à pouvoir fournir (authentification).Une fois l'authentification réussie, le login de l'utilisateur est attribué, à travers la table des utilisateurs authentifiés, à la machine à partir de laquelle celui-ci s'est identifié et à tous les paquets IP qui en proviennent, et ce pour une durée spécifiée par l'utilisateur. L'utilisateur peut également se retirer manuellement de la table des utilisateurs authentifiés avant cette échéance.

Pour cette section, vous devez avoir franchi les étapes

- ► Installation, pré-configuration, intégration,
- ► Définition des interfaces, des objets et de la configuration du noyau.

Pour cette section vous devez connaître

- ► Les données des utilisateurs (nom, prénom, adresse e-mail ...).

Utilité de la section

Cette section vous permettra de configurer la base de données des utilisateurs, de générer l'autorité de certification servant à créer les certificats numériques et de choisir la méthode d'authentification qu'utiliseront les utilisateurs internes.

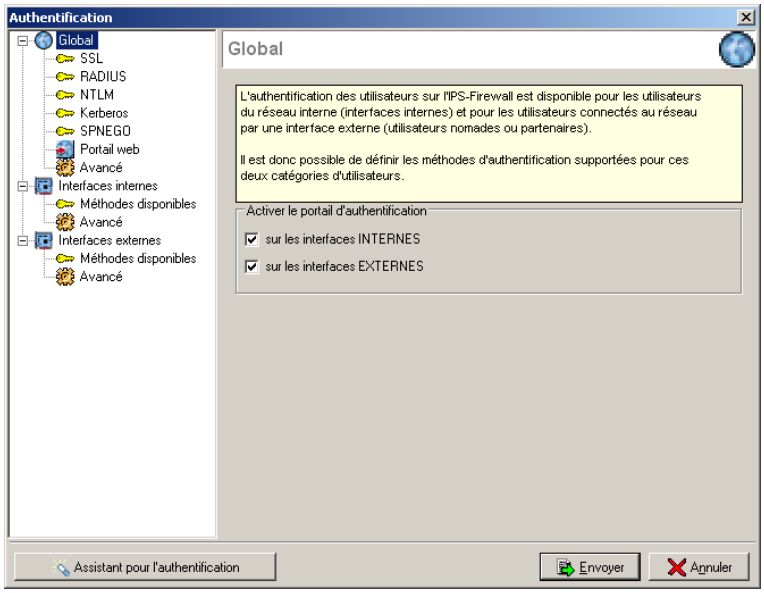
L'authentification utilise une base de données LDAP (Lightweight Directory Access Protocol) stockant des fiches utilisateurs et, éventuellement, le certificat numérique x509 de l'utilisateur. Chaque firewall NETASQ embarque une base de données LDAP mais vous avez aussi la possibilité d'utiliser une base LDAP externe. Ainsi, vous pourrez centraliser vos fiches utilisateurs sur une base LDAP externe et plusieurs firewalls pourront utiliser la même base. Les Firewalls NETASQ supportent aussi l'authentification via un serveur RADIUS, un serveur Kerberos ou un serveur NTLM externe.

NETASQ supporte aussi l'utilisation du protocole SRP pour l'authentification des utilisateurs. Ce protocole sans divulgation de mot de passe est résistant aussi bien aux attaques d'écoute passive qu'aux attaques actives basées sur la modification ou l'insertion de paquets dans la séquence d'authentification. Il utilise un mot de passe réutilisable fourni par l'utilisateur, et conserve ses propriétés de résistance aux attaques même lorsque l'entropie du mot de passe est basse.

Concrètement, l'IPS-Firewall fournit, à travers des capacités de type « serveur HTTP », des formulaires Web qui permettent de s'identifier, de s'authentifier en spécifiant la durée de la session, et de fermer la session manuellement. Il n'est pas nécessaire que la session HTTP persiste pour que la session reste active. Les étapes du protocole SRP sont effectuées par une applet Java téléchargée depuis l'IPS-Firewall sur le poste de l'utilisateur. Cette applet se sert du mot de passe fourni par l'utilisateur pour mener les étapes du protocole SRP. Grâce à cet enrôlement WEB, la tâche de l'administrateur est simplifiée car ce sont les utilisateurs qui demandent la création de leur compte d'accès (à l'Internet, au serveur mail, à tous les services qui nécessitent selon votre politique de filtrage une authentification) en renseignant eux-mêmes les informations les concernant.

© Copyright NETASQ 2006

Avant d'activer l'authentification, vous devez avoir configuré la base de données LDAP (Voir « Configuration de la base LDAP »). L'activation de l'authentification est accessible par le menu « Authentification > Général ».



L'écran de configuration de l'authentification se décompose en deux parties :

► A gauche un arbre présentant les diverses fonctionnalités du menu configuration de l'authentification,
► A droite les options configurables.

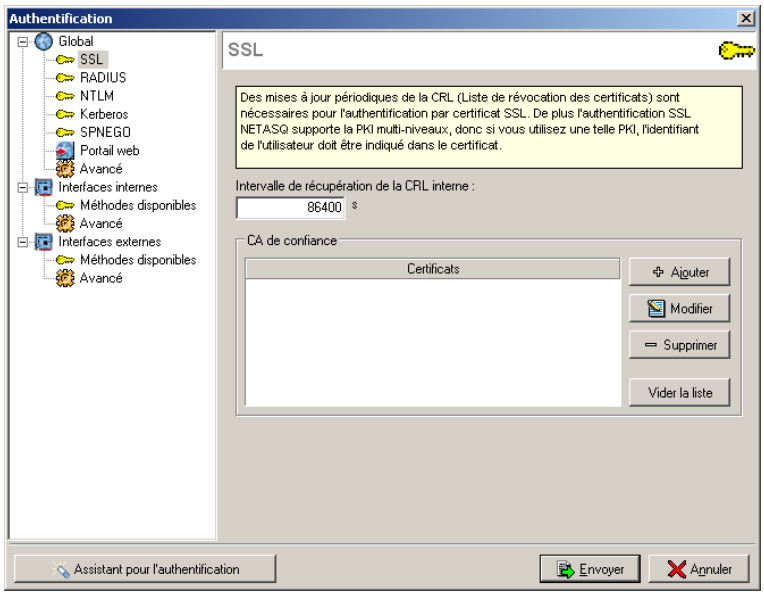
Global

L'authentification sur les IPS-Firewalls est différenciée par les interfaces sur lesquelles arrivent les flux de trafic. En effet il est possible d'activer l'authentification uniquement sur les interfaces internes, uniquement sur les interfaces externes ou sur les deux types d'interfaces.

Pour activer l'authentification sur un type d'interface, cochez l'option « Activer l'authentification sur les interfaces … » correspondant au type d'interface.

© Copyright NETASQ 2006

SSL



Lorsque la méthode SSL est sélectionnée, l'authentification SSL est activée. Les options de configuration de la méthode SSL sont indiquées dans le tableau ci-dessous :

Intervalle de récupération de la CRL interne	Temps en secondes au bout duquel il faut récupérer la CRL servant à vérifier la validité des certificats numériques créés par la PKI interne de l'IPS-Firewall.

CA de confiance

La méthode d'authentification SSL peut accepter l'utilisation de certificats signés par une autorité de certification externe à l'IPS-Firewall. Pour cela il est nécessaire d'ajouter cette autorité de certification dans la configuration de l'IPS-Firewall de façon à ce que celui accepte tous les certificats effectivement signés par cette autorité. Si l'autorité de certification est elle-même signée par une autre autorité de certification. Il est possible de rajouter cette autorité dans la liste des CA de confiance pour ainsi créer une « Chaîne de confiance ».

Lorsqu'une CA de confiance ou une chaîne de CA de confiance est spécifiée dans la configuration de la méthode d'authentification SSL, elle s'ajoute à la CA interne de l'IPS-Firewall implicitement vérifiée dès qu'il existe une PKI interne valide sur l'IPS-Firewall.

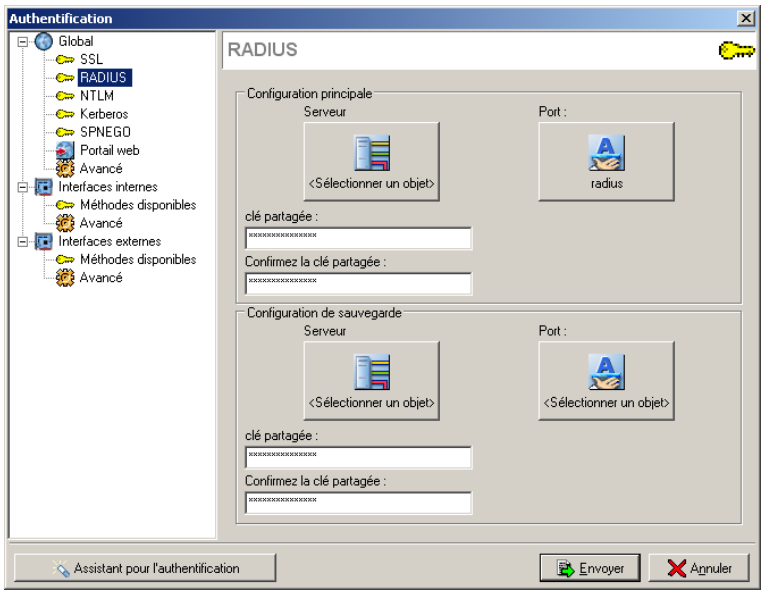
Ajouter	L'ajout d'une autorité de certification dans la liste des autorités de certification de confiance permet d'accepter cette autorité comme autorité reconnue et de valider tous les certificats signés par cette autorité de certification. En cliquant sur le bouton « Ajouter » on accède à la fenêtre des certificats externes. Si l'autorité de certifcation à laquelle vous desirez faire confiance ne fait pas partie de la liste des certificats externes, cliquez sur le bouton « Ajouter » de la fenêtre des certificats externes pour ajouter cette autorité de certification dans la liste. Les IPS-Firewalls supportent les PKI multiniveaux. Ainsi si le certificat de l'utilisateur à authentifier est signé par une autorité de certification, elle-même signée par une autorité de certification supérieure, vous pouvez insérer toute la chaine de certification créée par cette PKI multiniveaux. Pour que toute la chaîne soit correctement prise en compte, il est important d'insérer l'ensemble de la chaîne des autorités entre

	l'autorité la plus haute que vous avez inséré et l'autorité directement supérieure au certificat utilisateur.
Modifier	Permet la modification d'une autorité de certification. Par exemple, chaque CA est obligatoirement associée à une CRL. Cette CRL a une durée de vie limitée (pour prendre en compte régulièrement les nouveaux certificats révoqués) mais elle n'est pas modifiée automatiquement, il faut donc le faire manuellement.
Supprimer	Supprime l'autorité de certification sélectionnée.
Vider la liste	Supprime la liste complète des certificats configurés.

L'ajout d'une autorité de certification de confiance nécessite obligatoirement d'associer à cette CA, une liste de révocation des certificats. L'assistant d'ajout d'autorité de certification demande obligatoirement cet ajout. Toutefois cette CRL n'est pas récupérée automatiquement comme dans le cas de la CRL interne de la PKI des IPS-Firewalls NETASQ.

L'utilisation d'une autorité de certification externe nécessite que l'email spécifié dans le certificat utilisateur qui sera utilisé pour l'authentification soit identique à celui précisé dans la fiche utilisateur de la base d'utilisateur de l'IPS-Firewall. Afin que celui-ci puisse effectuer une correspondance stricte entre le certificat qui lui proposé et un identifiant d'utilisateur présent dans sa base d'utilisateurs.

Radius



Introduction

RADIUS est un protocole d'authentification qui fonctionne en mode client-serveur. Le firewall NETASQ peut se comporter comme un client RADIUS. Il peut alors adresser, à un serveur RADIUS externe, des demandes d'authentification pour les utilisateurs désirant traverser le firewall. L'utilisateur ne sera authentifié sur le firewall que si le RADIUS accepte la demande d'authentification envoyée par le firewall.

Toutes les transactions RADIUS (communications entre le firewall et le serveur RADIUS) sont elles-mêmes authentifiées par l'utilisation d'un secret pré-partagé, qui n'est jamais transmis sur le réseau. Ce même secret sera utilisé pour chiffrer le mot de passe de l'utilisateur, qui transitera entre le firewall et le serveur RADIUS. L'authentification RADIUS utilise le protocole UDP sur le port 1812.

Fonctionnement

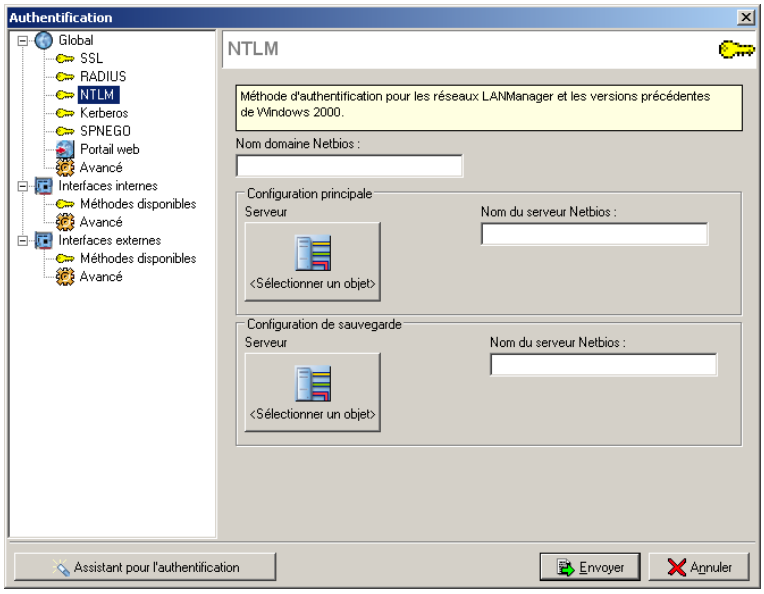
Lorsque la méthode RADIUS est sélectionnée, l'authentification RADIUS est activée. Ce menu vous permet de préciser les informations relatives au serveur RADIUS externe utilisé et d'un éventuel serveur RADIUS de sauvegarde. Pour chacun la configuration nécessite de renseigner les informations présentées dans le tableau suivant :

Serveur	Adresse IP du serveur RADIUS.
Port	Port utilisé par le serveur RADIUS.
Clef partagée	Clef utilisée pour le chiffrement des échanges entre l'IPS-Firewallet le serveur RADIUS.

Processus de basculement entre le serveur principal et le serveur de backup

L'IPS-Firewall tente de se connecter 2 fois au serveur RADIUS « principal », en cas d'échec il tente de se connecter 2 fois au serveur RADIUS « backup ». Si le serveur RADIUS « backup » répond, il bascule en tant que serveur RADIUS « principal ». Au bout de 600 secondes, un nouveau basculement s'opère, l'ancien serveur RADIUS « principal » redevient « principal ».

NTLM



Introduction

NTLM sert de protocole d'authentification pour les transactions entre deux ordinateurs d'un même domaine, où l'un des deux ordinateurs, ou les deux, exécutent Windows NT 4.0 ou une version précédente.

Le protocole de NTLM authentifie des utilisateurs et des ordinateurs basés sur un mécanisme de challenge / réponse. Toutes les fois qu'une nouvelle marque d'accès est nécessaire, le firewall entre en contact avec un service d'authentification sur le contrôleur de domaine pour vérifier l'identité de l'utilisateur.

L'utilisateur ne sera authentifié sur le firewall que si le service d'authentification NTLM accepte la demande d'authentification envoyée par le firewall.

L'IPS-Firewall est donc compatible avec l'authentification NT.

Fonctionnement

Lorsque la méthode NTLM est sélectionnée, l'authentification NTLM est activée. Ce menu vous permet de préciser les informations relatives au serveur NTLM externe utilisé et d'un éventuel

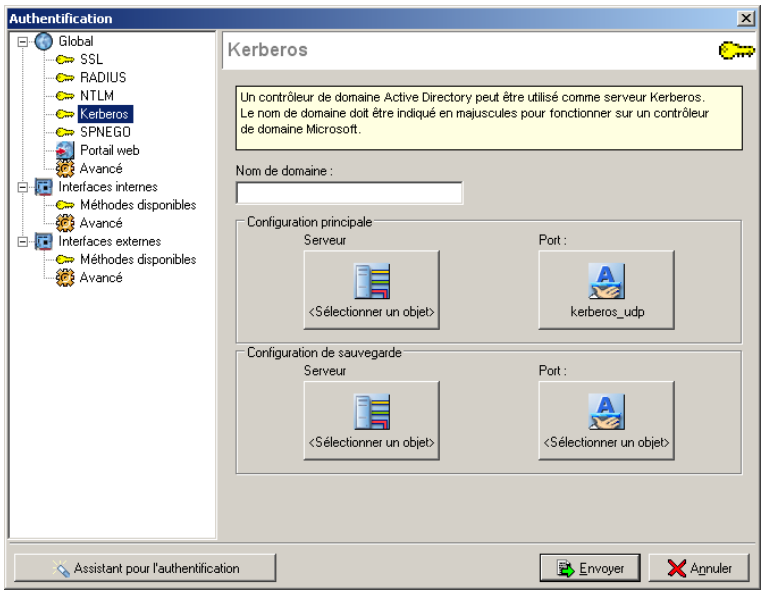
serveur NTLM de sauvegarde. Pour chacun la configuration nécessite de renseigner les informations présentées dans le tableau suivant :

Serveur	Adresse IP du serveur NTLM.
Nom Netbios du serveur	Nom utilisé par le serveur NTLM.
Nom de domaine Netbios	Nom de domaine sur lequel est utilisé le serveur NTLM.

Processus de basculement entre le serveur principal et le serveur de backup

L'IPS-Firewall tente de se connecter 2 fois au serveur NTLM « principal », en cas d'échec il tente de se connecter 2 fois au serveur NTLM « backup ». Si le serveur NTLM « backup » réponde, il bascule en tant que serveur NTLM « principal ». Au bout de 600 secondes, un nouveau basculement s'opère, l'ancien serveur RADIUS « principal » redevient « principal ».

Kerberos



Introduction

Kerberos est différent des autres méthodes d'authentification. Plutôt que de laisser l'authentification avoir lieu entre chaque machine cliente et chaque serveur, Kerberos utilise un cryptage symétrique et un programme fiable, le Centre distributeur de tickets (KDC, Key Distribution Center) afin d'authentifier les utilisateurs sur un réseau.

Une fois l'authentification effectuée, Kerberos stocke un ticket spécifique à cette session sur l'ordinateur de l'utilisateur et les services « kerberisés » rechercheront ce ticket au lieu de demander à l'utilisateur de s'authentifier à l'aide d'un mot de passe.

Dans ce processus d'authentification le firewall NETASQ agit comme un client qui se substitue à l'utilisateur pour demander une authentification. Cela signifie que même si l'utilisateur est déjà authentifié sur le KDC pour son ouverture de session Windows par exemple, il faut tout de même se ré-authentifier auprès de ce serveur même si les informations de connexion sont identiques, pour traverser le firewall.

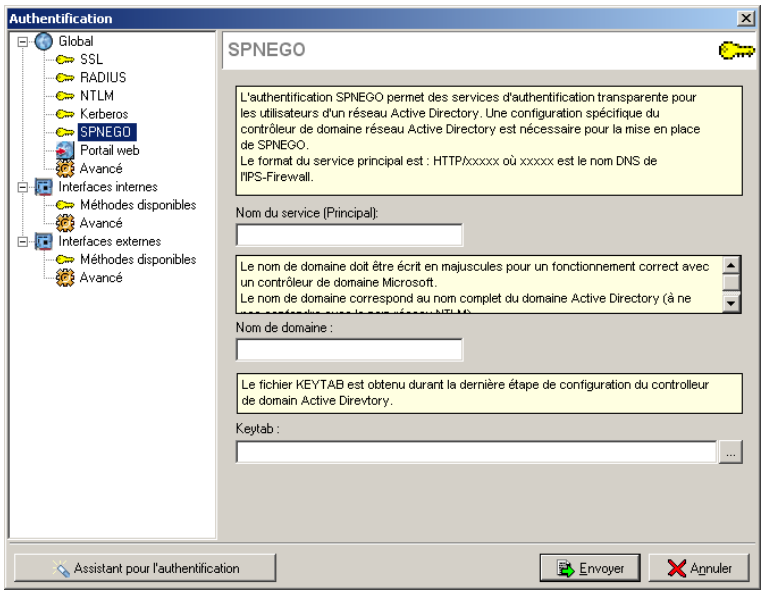
Toutefois l'intérêt de cette méthode est qu'il n'y a qu'une base d'authentification à tenir à jour. Kerberos est utilisé par les environnements Windows 2000 et XP, ce qui rend le firewall compatible avec l'authentification de ces systèmes.

Fonctionnement

Lorsque la méthode Kerberos est sélectionnée, l'authentification Kerberos est activée. Ce menu vous permet de préciser les informations relatives au serveur Kerberos externe utilisé et d'un éventuel serveur Kerberos de sauvegarde. Pour chacun la configuration nécessite de renseigner les informations présentées dans le tableau suivant :

Serveur	Adresse IP du serveur Kerberos.
Port	Port utilisé par le serveur Kerberos.
Nom de domaine	Nom de domaine sur lequel est utilisé le serveur Kerberos.

SPNEGO


Authentification
Global
SSL
RADIUS
NTLM
Kerberos
SPNEGO
Portail web
Avancé
Interfaces internes
Méthodes disponibles
Avancé
Interfaces externes
Méthodes disponibles
Avancé
SPNEGO
L'authentification SPNEGO permet des services d'authentification transparente pour les utilisateurs d'un réseau Active Directory. Une configuration spécifique du contrôleur de domaine réseau Active Directory est nécessaire pour la mise en place de SPNEGO.
Le format du service principal est : HTTP/xxxxx où xxxxx est le nom DNS de l'IPS-Firewall.
Nom du service (Principal):
Le nom de domaine doit être écrit en majuscules pour un fonctionnement correct avec un contrôleur de domaine Microsoft.
Le nom de domaine correspond au nom complet du domaine Active Directory (à ne
Nom de domaine :
Le fichier KEYTAB est obtenu durant la dernière étape de configuration du controlleur de domain Active Direvtory.
Keytab :
Assistant pour l'authentification
Envoyer
Annuler

Introduction

La méthode SPNEGO permet le fonctionnement du « Single Sign On » pour l'authentification WEB avec un serveur d'authentification externe Kerberos. Cela signifie qu'un utilisateur se connectant à son domaine par une solution basée sur un serveur Kerberos serait automatiquement authentifié sur un IPS-Firewall NETASQ dans le cas d'un accès à l'Internet (nécessitant une authentification dans la politique de filtrage sur l'IPS-Firewall) grâce à un navigateur WEB (Internet Explorer, Firefox, Mozilla).

Prérequis

La solution NETASQ s'intègre dans le cadre d'une solution de Single Sign On complète, il s'agit donc d'installer certains composants sur le serveur Kerberos. Pour cela suivez la procédure suivante :

1. Installation d'un « Service Principal Name » (SPN) sur le serveur Kerberos afin de permettre le chiffrement des échanges entre le serveur Kerberos, l'utilisateur et l'IPS-Firewall,

2. Exécuter le script SPNEGO livré par NETASQ dans le CDROM de l'Administration Suite,

3. Récupérer la « KeyTab » générée par le script.

Fonctionnement

La configuration de SPNEGO sur l'IPS-Firewall est réalisée grâce aux options expliquées dans le tableau suivant :

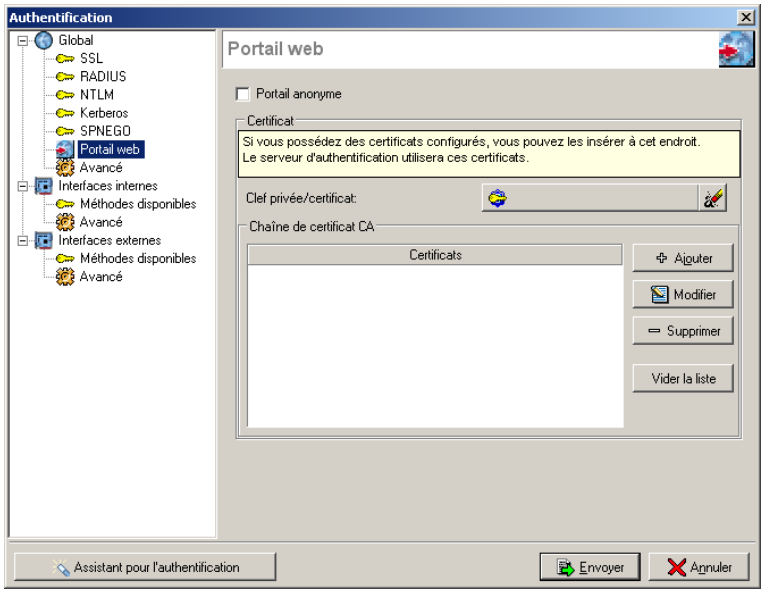
Nom du service (Principal)	Nom ou adresse de l'IPS-Firewall utilisé pour l'authentification. Ce nom correspond au nom indiqué dans le script NETASQ (voir

	ci-dessus). Il sera précédé de la mention « HTTP/ ». Exemple : HTTP/F200XA099999999999.
Nom de domaine	Nom de domaine du serveur Kerberos. Ce nom de domaine correspond au nom de domaine indiqué dans le script.
KeyTab	Récupérer la « KeyTab » générée par le script NETASQ (voir ci-dessus).

Pour réaliser une redirection transparente de l'authentification, activez le proxy HTTP (Voir « Configuration du proxy HTTP »).

Notez que l'authentification WEB ne s'active que si une règle d'authentification a été définie dans la politique de filtrage (Voir « Configuration du filtrage »).

Portail WEB



Portail anonyme	Lorsque cette option est activée, le logo NETASQ du portail d'authentification est masqué.
Clé privée	Par défaut le certificat utilisé par le module d'authentification de l'IPS-Firewall est le certificat propre de l'IPS-Firewall, le nom associé à ce certificat est le numéro de série du produit. Ainsi lorsqu'un utilisateur essaie de contacter l'IPS-Firewall différemment que par son numéro de série, il reçoit un message d'avertissement indiquant une incohérence entre ce que l'utilisateur essaie de contacter et le certificat qu'il reçoit. Pour éviter ce message, le module d'authentification des IPS-Firewalls offre la possibilité de spécifier un certificat « serveur » (impossible de spécifier un certificat utilisateur pour cette fonctionnalité) dont le nom serait beaucoup plus facile à retenir. Par exemple : www.netasq.com. Pour obtenir ce type de certificat, vous devez contacter des organismes du type Verisign ou Thawte.

Chaîne de certificat CA

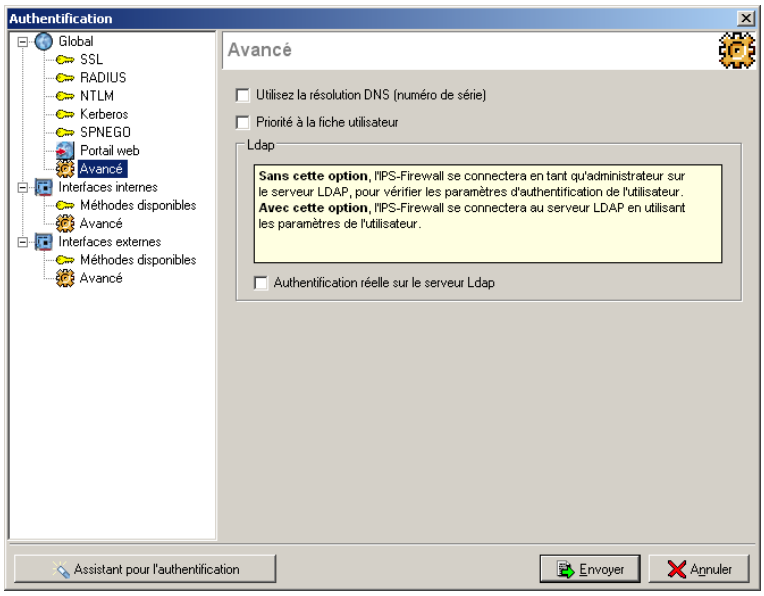
Cette chaîne de certificat CA certifie la clé privée utilisée dans la configuration du portail d'authentification. Pour cela il est nécessaire d'ajouter cette autorité de certification dans la configuration de l'IPS-Firewall de façon à ce que celui accepte tous les certificats effectivement signés par cette autorité (et la clé privée spécifiée plus haut plus particulièrement. Si l'autorité de

certification est elle-même signée par une autre autorité de certification. Il est possible de rajouter cette autorité dans la liste des CA de confiance pour ainsi créer une « Chaîne de confiance ».

Ajouter	L'ajout d'une autorité de certification dans la liste des autorités de certification de confiance permet d'accepter cette autorité comme autorité reconnue et de valider tous les certificats signés par cette autorité de certification. En cliquant sur le bouton « Ajouter » on accède à la fenêtre des certificats externes. Si l'autorité de certifcation à laquelle vous desirez faire confiance ne fait pas partie de la liste des certificats externes, cliquez sur le bouton « Ajouter » de la fenêtre des certificats externes pour ajouter cette autorité de certification dans la liste. Les IPS-Firewalls supportent les PKI multiniveaux. Ainsi si le certificat de l'utilisateur à authentifier est signé par une autorité de certification, elle-même signée par une autorité de certification supérieure, vous pouvez insérer toute la chaine de certification créée par cette PKI multiniveaux. Pour que toute la chaîne soit correctement prise en compte, il est important d'insérer l'ensemble de la chaîne des autorités entre l'autorité la plus haute que vous avez inséré et l'autorité directement supérieure au certificat utilisateur.
Modifier	Permet la modification d'une autorité de certification. Par exemple, chaque CA est obligatoirement associée à une CRL. Cette CRL a une durée de vie limitée (pour prendre en compte régulièrement les nouveaux certificats révoqués) mais elle n'est pas modifiée automatiquement, il faut donc le faire manuellement.
Supprimer	Supprime l'autorité de certification sélectionnée.
Vider la liste	Supprime la liste complète des certificats configurés.

L'ajout d'une autorité de certification de confiance nécessite obligatoirement d'associer à cette CA, une liste de révocation des certificats. L'assistant d'ajout d'autorité de certification demande obligatoirement cet ajout. Toutefois cette CRL n'est pas récupérée automatiquement comme dans le cas de la CRL interne de la PKI des IPS-Firewalls NETASQ.

Avancé



Utilisez la résolution DNS (N° série)

Lorsque l'authentification transparente est activée (utilisation du proxy URL), l'utilisateur désirant se connecter à un site WEB doit d'abord s'authentifier en HTTPS sur le Firewall. Pour cela, le navigateur de l'utilisateur vérifie le certificat du firewall. Un message d'erreur s'affiche dans le navigateur puisque le certificat correspond au numéro de série du firewall et pas à son adresse IP. L'utilisation de la résolution DNS permet de faire la correspondance entre le numéro de série du firewall et son adresse IP.

Il faut, dans ce cas, que le numéro de série du firewall soit indiqué au niveau du serveur DNS. (Correspondance entre le numéro de série du firewall et son adresse IP).

Authentification réelle sur le serveur LDAP

Lorsque cette option est décochée, l'IPS-Firewall réalise une connexion en temps qu'administrateur sur le serveur LDAP pour valider l'authentification de l'utilisateur.

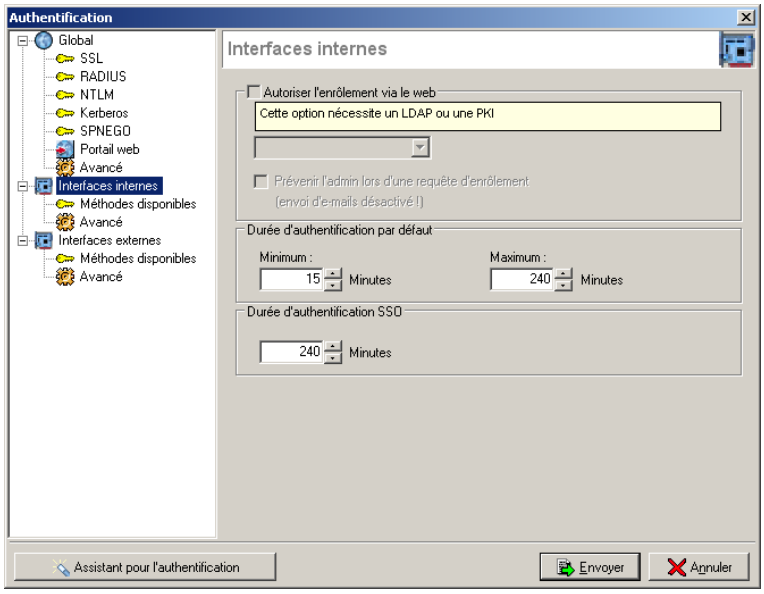
Lorsque cette option est cochée, l'IPS-Firewall tente réellement de s'authentifier sur le serveur LDAP avec les paramètres de l'utilisateur. Si l'authentification de l'IPS-Firewall sur le serveur LDAP échoue, l'authentification est alors refusée à l'utilisateur.

Priorité à la fiche utilisateur

Lorsque cette option est cochée, quel que soit le résultat de la méthode d'authentification SPNEGO, l'IPS-Firewall tentera une authentification grâce à la méthode indiquée dans la fiche de l'utilisateur.

Interface interne et interface externe

Pour chaque type d'interface, l'activation de l'authentification nécessite la définition de paramètres d'utilisation. Ces paramètres d'utilisation sont les mêmes pour les interfaces dites internes (**ne possédant pas** l'attribut « Externe » dans la configuation réseau) et pour les interfaces dites externes (possédant l'attribut « Externe » dans la configuration réseau).



Autoriser l'enrôlement via le web

NETASQ vous propose l'enrôlement d'utilisateurs par le web. Si l'utilisateur qui tente de se connecter n'existe pas dans la base des utilisateurs, il a la possibilité de demander la création de son compte par un enrôlement WEB.

Liste déroulante	Vous pouvez spécifier deux types d'enrôlement disponible à partir du web : ► LDAP : création d'un compte utilisateur, ► LDAP/PKI : création d'un compte utilisateur et d'un certificat.
Envoi des requêtes par e-mail	Lorsqu'un utilisateur demande la création d'un compte par l'enrôlement WEB, cette requête est indiquée dans le firewall manager. L'administrateur peut aussi être prévenu de cette requête par mail si l'option « Envoi des requêtes par e-mail » est cochée. Dans ce cas le firewall NETASQ utilise l'adresse e-mail indiquée dans la configuration des traces (Voir Chapitre VIII).

Durée d'authentification

Minimum	Temps minimum durant lequel l'utilisateur est authentifié.
Maximum	Temps maximum durant lequel l'utilisateur est authentifié. Au bout de ce délai, l'authentification expire et l'utilisateur doit se ré-authentifier.

Les deux précédentes valeurs permettent de définir une plage de choix pour l'authentification (l'utilisateur pourra choisir une durée d'authentification comprise dans cette plage).

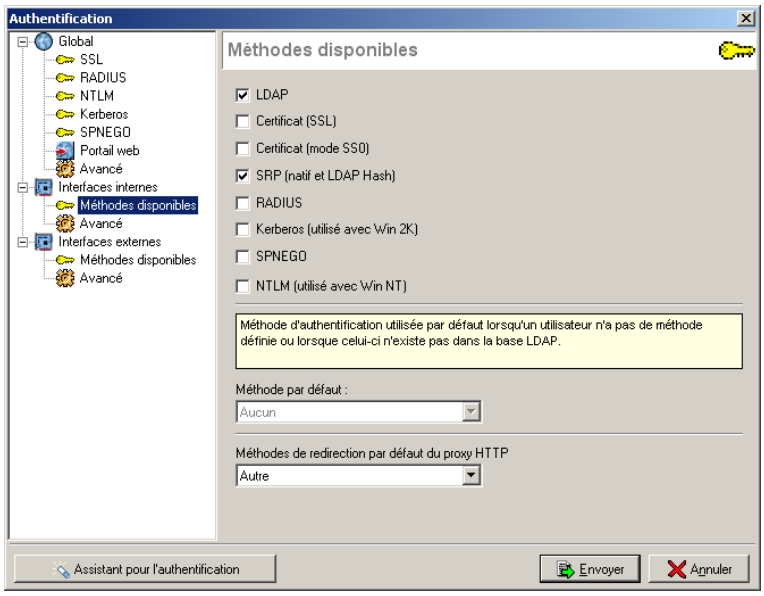
Afin d'éviter le détournement de session d'authentification, il est conseillé de ne pas définir un temps maximum trop élevé (4 heures maximum) mais cela implique que l'utilisateur devra se ré-authentifier souvent.

Durée d'authentification SSO

Lorsqu'une méthode d'authentification basée sur SSO (Signle Sign On), l'authentification unique, cette période permet de définir la durée pendant laquelle aucune ré-authentification transparente n'est de demandée par l'IPS-Firewall.

© Copyright NETASQ 2006

Méthodes disponibles



Choisissez la ou les méthodes autorisées sur l'IPS-Firewall NETASQ. Ces méthodes correspondent à des mécanismes d'authentification différents. Chaque utilisateur peut avoir une méthode d'authentification différente mais elle doit avoir été sélectionnée dans cette fenêtre pour être utilisable.

LDAP	L'utilisateur doit saisir un couple login/mot de passe. Ces informations transitent en SSL (si l'utilisateur se connecte au firewall en https avec son navigateur Internet). Cette méthode utilise le port 443. **Cette méthode est la moins sécurisée car il est désormais possible d'accéder (frauduleusement) aux informations contenues dans un trafic SSL. Toutefois cela ne s'applique à la méthode SSL+Certificat.**
Certificat (SSL)	L'utilisateur n'a pas besoin de saisir de couple login/mot de passe mais un certificat numérique généré par la PKI interne du firewall doit être installé sur le poste utilisateur. Les informations sont chiffrées en SSL. L'utilisateur doit, pour s'authentifier, se connecter au firewall en https avec son navigateur Internet. Cette méthode utilise le port 443.
Certificat (Mode SSO)	Basée sur une utilisation de la méthode SSL dans un mode SSO (Single Sign On) permet la simplication des étapes d'authentification par la méthode SSL. En effet l'IPS-Firewall reconnaît automatiquement la méthode d'authentification qui sera utilisée pour l'authentification de l'utilisateur.
SRP	Cette méthode utilise le protocole SRP (Secure Remote Password) pour lequel le mot de passe n'est jamais émis. L'utilisateur doit se connecter au firewall en https et saisir un couple login/mot de passe. Cette méthode utilise les ports 443 et 1200 (port utilisé par l'applet Java SRP). Cette méthode inclue le SRP natif et le SRP_Hash.
Radius	Cette méthode est utilisée si l'authentification est relayée à un serveur RADIUS externe.
Kerberos Win2k	Cette méthode est utilisée si l'authentification est relayée à un serveur Kerberos externe.

SPNEGO	Cette méthode utilise le principe d'authentification unique permettant dans certaines conditions que lorsque l'utilisateur est authentifié sur un domaine grâce à l'ouverture de sa session, il soit aussi authentifié auprès de l'IPS-Firewall.
NTLM WinNT	Cette méthode est utilisée si l'authentification est relayée à un serveur NTLM externe.

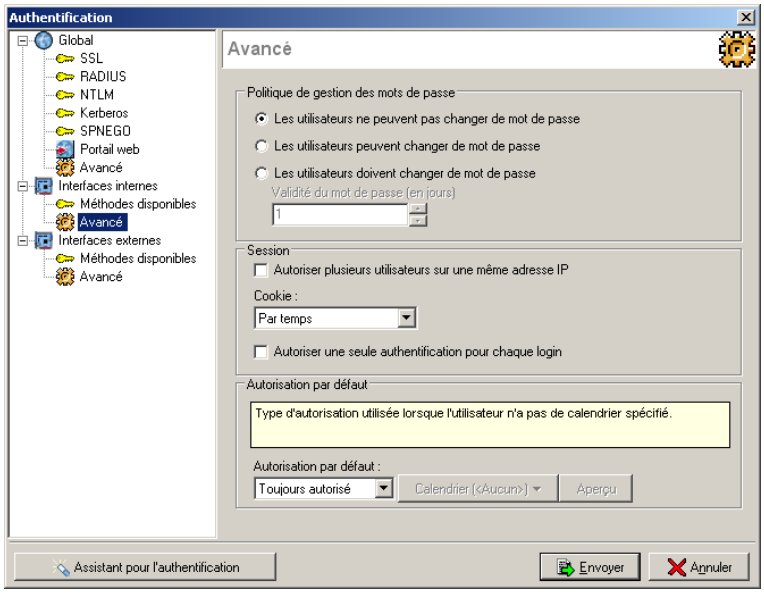
Méthode par défaut

Cette méthode est utilisée lorsqu'un utilisateur désirant s'authentifier n'est pas présent dans l'annuaire LDAP interne ou externe. Cette option vous permet, par exemple, d'avoir certaines fiches utilisateurs sur la base LDAP et d'autres sur un serveur RADIUS, Kerberos ou NTLM (dans ce cas, sélectionnez les options correspondantes). Par exemple, si on sélectionne RADIUS, lorsqu'un utilisateur n'est spécifié dans la base LDAP, le firewall interrogera le serveur RADIUS.

Méthode de redirection par défaut du proxy HTTP

Lorsqu'une méthode de redirection par défaut du proxy HTTP est activé (SRP, Certificat ou SPNEGO), le mode SSO de cette méthode est activé. Par exemple dans le cas de la méthode d'authentification SRP en mode SSO, l'applet SRP du portail d'authentification présente le login et le mot de passe sur la page. En effet car quelles que soit les méthodes d'authentification c'est la méthode SRP en mode SSO qui sera utilisée.

Avancé



Politique de mots de passe utilisateurs

Il existe trois possibilités de gestion des mots de passe utilisateurs sur les IPS-Firewalls NETASQ.

► Les utilisateurs ne peuvent pas changer de mot de passe : en sélectionnant cette option, il sera impossible aux utilisateurs de modifier leur mot de passe d'authentification sur l'IPS-Firewall NETASQ ;

► Les utilisateurs peuvent changer de mot de passe : en sélectionnant cette option, les utilisateurs peuvent modifier leur mot de passe d'authentification sans contrainte de temps et de validité ;

► Les utilisateurs doivent changer de mot de passe : en sélectionnant cette option, les utilisateurs doivent changer leur mot de passe d'authentifcation à leur première connexion sur le portail d'authentifcation de l'IPS-Firewall puis à chaque fois que la durée de validité du mot de passe est expiré. Cette durée est spécifiée en jours sans précision d'heure. Cela signifie que par exemple si la durée de validité du mot de passe de l'utilisateur est de 1 jour

et que le mot de passe de l'utilisateur est initialisé une première fois le 27 juillet 2005 14:00, ce mot de passe doit être modifié dès le 28 juillet 2005 00:00 et non 24 heures plus tard.

Session

La section « Session » de la configuration de l'authentification est composé de trois options expliquées dans le tableau suivant :

Plusieurs logins sur la même adresse IP	L'authentification NETASQ est basée sur l'enregistrement dans une table de l'ASQ d'une entrée qui associe un nom d'utilisateur à une adresse IP. Par défaut, il est impossible d'enregistrement plusieurs logins sur la même adresse IP. En cochant cette option, il est possible d'enregistrer plusieurs logins sur la même adresse IP permettant ainsi l'authentification d'utilisateurs différents situés derrière un équipement de NAT qui masquerait l'adresse réelle des utilisateurs par une adresse IP unique.
Cookie	La gestion des cookies pour l'authentification des utilisateurs sur les IPS-Firewalls permet une sécurisation de l'authentification prévenant par exemple les attaques par rejeu étant donné qu'il est indispensable de posséder le cookie de connexion pour être considéré comme authentifié. Par défaut les cookies sont définis « par Temps », ce qui signifie que les cookies sont négociés qu'une seule fois pour toute la duréee d'authentification. Mais il est aussi possible de configurer les cookies « par Session », ce qui signifie que les cookies sont négociés à chaque instance du navigateur WEB. Enfin il est possible de ne pas utiliser les cookies, mais cette option n'est pas recommandée car elle dégrade la sécurité de l'authentification. Les cookies sont indispensables pour le fonctionnement de l'option « Plusieurs logins sur la même adresse IP ». Les cookies sont négociés par navigateur WEB. Ainsi si une authentification est réalisée avec Internet Explorer, elle ne sera pas effective avec Firefox ou d'autres navigateurs WEB.
Un seul login sur une seule adresse IP	En cochant cette option, il est impossible pour un utilisateur de s'authentifier deux fois sur deux machines différentes.

Autorisation par défaut

Lorsqu'un utilisateur est créé ou lorsque des règles d'authentification le concernant sont mises en place, on associe à cet utilisateur un calendrier (Chapitre IV Section D Programmation Horaire). Ce dernier spécifie les zones horaires où l'utilisateur a le droit de s'authentifier. Pour toutes les autres zones, la connexion est refusée.

Dans le cas où aucun calendrier ne correspond à un utilisateur, vous pouvez configurer plusieurs actions :

Toujours autorisé	L'utilisateur peut se connecter à toutes les heures, tous les jours définis par les règles de filtrage.
Toujours interdit	Quel que soit le résultat de l'authentification, la connexion est refusée.
Personnalisé	Vous avez la possibilité de spécifier un calendrier par défaut

Introduction

LDAP (Lightweight Directory Access Protocol) est un protocole standard permettant de gérer des annuaires, c'est-à-dire d'accéder à des bases d'informations sur les utilisateurs d'un réseau par l'intermédiaire de protocoles TCP/IP.

Le protocole LDAP définit la méthode d'accès aux données sur le serveur au niveau du client, et non la manière selon laquelle les informations sont stockées. Il présente les informations sous forme d'une arborescence d'informations hiérarchique appelée DIT (Directory Information Tree), dans laquelle les informations, appelées entrées (ou encore DSE, Directory Service Entry), sont représentées sous forme de branches.

Une branche située à la racine d'une ramification est appelée racine ou suffixe (en anglais root entry).

Chaque entrée de l'annuaire LDAP correspond à un objet abstrait ou réel (par exemple une personne, un objet matériel, des paramètres, ...).

Chaque entrée est constituée d'un ensemble de paires clés/valeurs appelées attributs.

Utilisation de LDAP dans les firewalls NETASQ

Les Firewalls NETASQ embarquent, depuis la version 4.0 du firmware, une base LDAP (Lightweight Directory Access Protocol) interne. Cette base permet de stocker les informations relatives aux utilisateurs devant s'authentifier pour passer au travers du firewall.

Assistant LDAP

L'assistant LDAP vous permettra de configurer facilement votre base de données LDAP.

Etape 1

Cette première étape de l'assistant de configuration de la base LDAP est accessible par le sous-menu « Authentification > Annuaire LDAP » lorsque la base LDAP n'est pas initialisée ou par un bouton sur l'écran de la configuration générale lorsque la Base LDAP est déjà initialisée.

Lors de cette première étape, vous devez choisir si vous désirez créer un annuaire LDAP interne au firewall ou alors indiquer au firewall d'utiliser un annuaire externe que vous possédez déjà.

En fonction de votre choix, l'étape suivante est variable, la configuration d'un LDAP externe réclamant plus de renseignements.

Etape 2 : Annuaire interne

Lors de cette seconde étape, vous devez renseigner les informations générales concernant la base LDAP que vous désirez créer. Les informations saisies se retrouveront dans le schéma de l'annuaire LDAP de votre IPS-Firewall.

© Copyright NETASQ 2006

Nom de la société (o)	le nom de votre société (ex : NETASQ).
Pays domaine (dc)	le domaine de votre société (ex : com).
Mot de passe d'administration LDAP	un mot de passe permettant au firewall de se connecter sur l'annuaire LDAP.
Rendre le LDAP public	Il est possible d'accéder de l'extérieur à l'annuaire LDAP. Deux méthodes sont disponibles : soit un accès en clair, soit un accès au moyen d'une authentification par Certificat (SSL). Il faut alors dans ce cas choisir le certificat désiré.

Remarque : seul le mot de passe sera modifiable par la suite.

Si l'accès externe n'est pas nécessaire, il est vivement conseillé de ne pas activer l'option « Rendre le LDAP public ».

Etape 2 : Annuaire externe

Dans certaines architectures, l'utilisation d'une base d'utilisateurs exploitable uniquement par le firewall peut devenir très rapidement trop contraignant. En effet, cela nécessite la gestion de multiples bases et une duplication manuelle des informations entre chacune des bases, les comptes utilisateurs ne sont pas centralisés. Ensuite, avec une base hermétique, il n'est pas possible de réutiliser les comptes utilisateurs déjà configurés sur d'autres bases.

Afin de remédier à cette limitation, les firewalls NETASQ offrent la possibilité de s'interfacer à des bases LDAP externes pour une intégration complète au sein du système d'information.

Lors de cette seconde étape, vous devez renseigner les informations générales concernant la base LDAP que vous possédez et que le firewall va consulter.

Cet assistant est décomposé en trois zones :

Configuration réseau du serveur LDAP externe :

Vous devez choisir un objet correspondant à votre serveur LDAP. Cet objet doit être créé au préalable et référencer l'adresse IP de votre serveur LDAP. Le choix du nom de l'objet doit correspondre au Common Name du certificat de votre serveur LDAP dans le cas de l'utilisation du protocole SSL, sinon, le nom de l'objet a peu d'importance.

Vous devez renseigner le port d'écoute de votre serveur LDAP. Les ports par défaut sont :

- 389 pour une authentification en clair,
- 636 pour une authentification en SSL.

Remarque : Pour que le firewall NETASQ puisse utiliser un annuaire LDAP externe, il faut que cet annuaire intègre le schéma LDAP NETASQ. Pour intégrer ce schéma, contactez le support technique de NETASQ.

Configuration de la sécurité des communications :

Si votre serveur LDAP est configuré pour supporter le SSL et que vous désirez que le firewall communique via SSL avec votre serveur vous devez cocher la case "Activer le SSL". Vous pouvez en option (en cochant la case "Envoyer un certificat au firewall" et en choisissant un fichier contenant le certificat de l'autorité) envoyer au firewall le Certificat de l'autorité ayant émis le certificat de votre serveur. Cela permet de vérifier la validité du certificat présenté par le serveur LDAP.

Configuration de la base LDAP

Base Dn	Vous devez renseigner le DN de la racine de votre annuaire (ex : o=NETASQ,dc=COM).

CA Dn	Ce champ est optionnel est sera uniquement utilisé si vous activez la PKI sur le firewall. Dans ce cas, le certificat et la CRL de l'autorité qui sera créée seront mis dans cette « fiche » LDAP. (ex : cn=Autorite Interne,ou=Autoritees de Certification).
Login	Un compte administrateur permettant au firewall de se connecter sur votre serveur LDAP et d'effectuer des lectures/écritures sur certains champs. Nous vous recommandons de créer un compte spécifique pour le firewall et de lui attribuer les droits uniquement sur les champs qui lui sont nécessaires. (ex : cn=Admin Firewall NETASQ).
Mot de passe	Le mot de passe pour permettre à l'utilisateur créé sur le firewall de se connecter sur le serveur LDAP.

Etape 2 : Active directory (base Windows 2000 ou XP)

Lors de cette seconde étape, vous devez renseigner les informations générales concernant la Base Active Directory que vous possédez et que le firewall va consulter.

Cet assistant est décomposé en trois zones :

Contrôleur de domaine

Vous devez choisir un objet correspondant à votre serveur Active Directory. Cet objet doit être créé au préalable et référencer l'adresse IP de votre serveur.

Nom de domaine

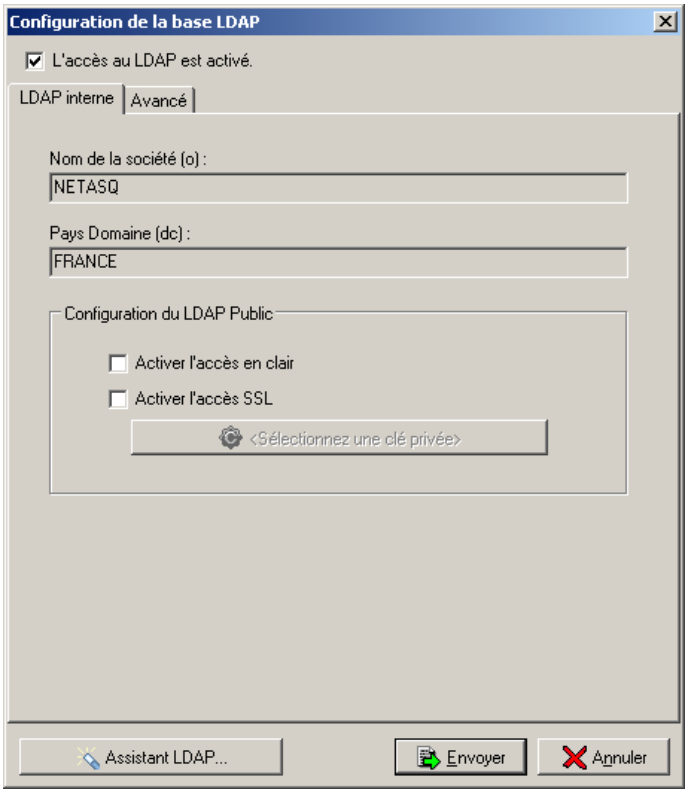
Vous devez renseigner le nom de domaine correspondant à la base Active Directory.

Configuration de la base Active Directory

Login	Un compte administrateur permettant au firewall de se connecter sur votre serveur Active Directory et d'effectuer des lectures/écritures sur certains champs. Nous vous recommandons de créer un compte spécifique sur la base Active Directory pour le firewall et de lui attribuer les droits uniquement sur les champs qui lui sont nécessaires. (ex : cn=Admin Firewall NETASQ).
Mot de passe	Le mot de passe pour permettre à l'utilisateur créé sur le firewall de se connecter sur le serveur Active Directory.

Une fois l'assistant utilisé, vous pouvez accèder à chacun des écrans de configuration

Onglet LDAP interne (si vous avez configuré un LDAP interne)



L'écran de configuration de la base LDAP interne est accessible par le sous-menu « Authentification > Annuaire LDAP ». Il vous permet de visualiser et de configurer votre base LDAP interne.

Il se décompose en trois parties :

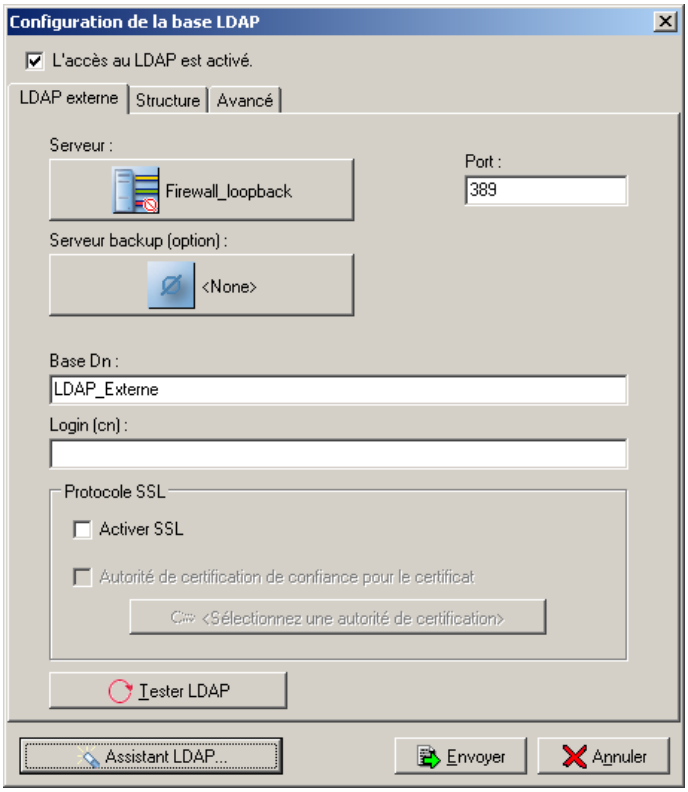
► une case à cocher indiquant le statut actuel de l'accès à l'annuaire LDAP. Si la case est cochée l'accès est actuellement actif, sinon, vous pouvez cocher cette case pour l'activer. Cela permet d'activer et de désactiver l'accès à l'annuaire LDAP sans pour autant détruire la configuration.

► une zone d'onglet et la fenêtre correspondant à l'onglet choisi. Les onglets disponibles vous permettent respectivement de :

► Visualiser la configuration actuelle de la base LDAP,
► Visualiser et modifier les paramètres avancés de votre configuration.

► une zone en bas à droite avec trois boutons vous permettant d'initialiser votre annuaire LDAP, d'envoyer vos modifications à l'IPS-Firewall ou de quitter cette fenêtre sans prendre en compte les modifications.

Onglet LDAP externe (pour un LDAP externe ou Active Directory)



Configuration réseau du serveur LDAP externe :

Vous devez choisir un objet correspondant à votre serveur LDAP. Cet objet doit être créé au préalable et référencer l'adresse IP de votre serveur LDAP. Le choix du nom de l'objet doit correspondre au Common Name du certificat de votre serveur LDAP dans le cas de l'utilisation du protocole SSL, sinon, le nom de l'objet a peu d'importance.

Vous devez renseigner le port d'écoute de votre serveur LDAP. Les ports par défaut sont :

- ► 389 pour une authentification en clair,
- ► 636 pour une authentification en SSL.

Il est possible de configurer un serveur de Backup externe. La configuration de serveur de backup est soumise aux mêmes exigences de configuration que le serveur LDAP externe « principal ».

Configuration de la sécurité des communications :

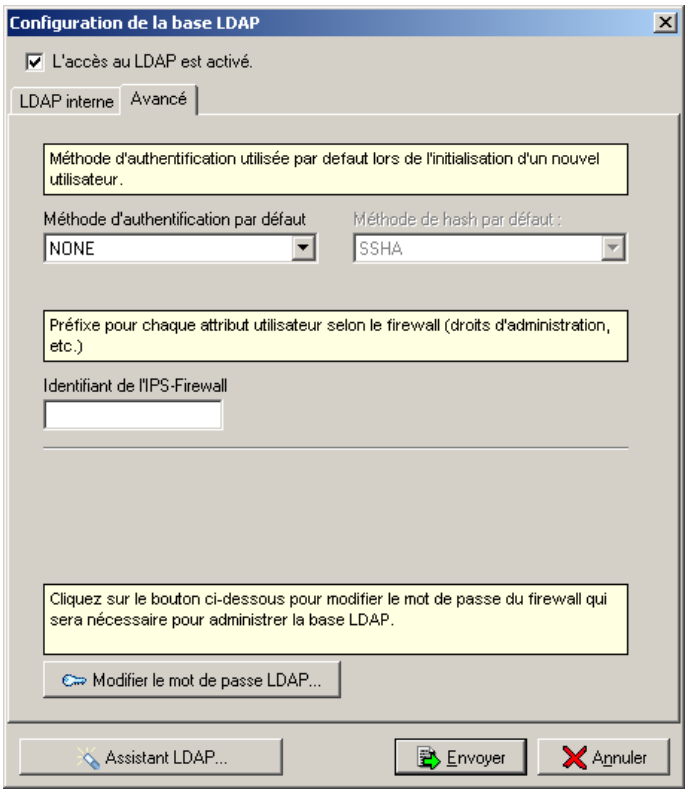
Si votre serveur LDAP est configuré pour supporter le SSL et que vous désirez que le firewall communique via SSL avec votre serveur vous devez cocher la case "Activer SSL". Vous pouvez en option (en cochant la case "Autorité de certification de confiance pour le certificat" et en choisissant un fichier contenant le certificat de l'autorité) envoyer au firewall le Certificat de l'autorité ayant émis le certificat de votre serveur. Cela permet de vérifier la validité du certificat présenté par le serveur LDAP.

Configuration de la base LDAP

Base Dn	Vous devez renseigner le DN de la racine de votre annuaire (ex : o=NETASQ,dc=COM).
Login	Un compte administrateur permettant au firewall de se connecter sur votre serveur LDAP et d'effectuer des lectures/écritures sur certains champs. Nous vous recommandons de créer un compte spécifique pour le firewall et de lui attribuer les droits uniquement sur les champs qui lui sont nécessaires. (ex : cn=Admin Firewall NETASQ).

Le bouton « Tester LDAP » permet de vérifier que le LDAP externe est bien accessible.

Onglet Avancé (pour un LDAP interne)


Configuration de la base LDAP
L'accès au LDAP est activé.
LDAP interne
Avancé
Méthode d'authentification utilisée par defaut lors de l'initialisation d'un nouvel utilisateur.
Méthode d'authentification par défaut
Méthode de hash par défaut :
NONE
SSHA
Préfixe pour chaque attribut utilisateur selon le firewall (droits d'administration, etc.)
Identifiant de l'IPS-Firewall
Cliquez sur le bouton ci-dessous pour modifier le mot de passe du firewall qui sera nécessaire pour administrer la base LDAP.
Modifier le mot de passe LDAP...
Assistant LDAP...
Envoyer
Annuler

Cet onglet permet de configurer les paramètres d'authentification des utilisateurs qui seront créés par la suite et de modifier le mot de passe de l'administrateur de la base LDAP.

Les différentes méthodes d'authentification disponibles sont les suivantes :

► NONE : les utilisateurs ne pourront pas s'authentifier,

► LDAP : l'authentification sera effectuée par transmission au firewall du mot de passe de l'utilisateur via un tunnel protégé (HTTPS) ou directement (HTTP),

► SSL : les utilisateurs devront présenter au firewall un certificat valide pour s'authentifier,

► SRP : cette méthode permet la non transmission du mot de passe utilisateur au firewall, elle est basée sur un protocole de défi-réponse,

► SRP_LDAP : cette méthode est identique à la précédente, à ceci près qu'elle utilise le mot de passe LDAP existant de l'utilisateur pour générer une clé éphémère SRP et permettre l'authentification SRP,

► RADIUS : cette méthode permet d'authentifier les utilisateurs sur un serveur RADIUS. Le mot de passe est transmis au firewall de la même manière que pour la méthode LDAP,

► Kerberos : cette méthode permet d'authentifier les utilisateurs sur un serveur Kerberos,

► NTLM : cette méthode permet d'authentifier les utilisateurs sur un serveur NTLM.

La méthode d'authentification SRP est l'une des plus sécurisées, nous vous en recommandons l'utilisation. La méthode d'authentification SRP_LDAP est très intéressante

lorsque l'annuaire LDAP est externe et que les utilisateurs possèdent déjà un mot de passe. Dans ce cas, elle permet d'obtenir une grande sécurité sans modifier l'existant.

Certaines méthodes d'authentification (SRP_LDAP,LDAP) doivent stocker le mot de passe utilisateur sous la forme d'un hash (résultat d'une fonction de hachage appliquée au mot de passe) qui évite le stockage en clair de ce mot de passe. Dans ce cas, vous devez choisir la méthode de hash désirée :

► NONE : pas de hash, le mot de passe est stocké en clair (Peu recommandé),

► MD5 : le mot de passe est hashé avec l'algorithme MD5,

► SMD5 : le mot de passe est hashé avec l'algorithme Salt MD5. Cette variante du MD5 utilise une valeur aléatoire pour diversifier l'empreinte du mot de passe. Deux mots de passe identiques auront ainsi deux empreintes différentes,

► SHA : le mot de passe est hashé avec l'algorithme SHA-1,

► SSHA : le mot de passe est hashé avec l'algorithme Salt SHA-1. Cette variante du SHA-1 utilise une valeur aléatoire pour diversifier l'empreinte du mot de passe. Deux mots de passe identiques auront ainsi deux empreintes différentes,

► CRYPT : le mot de passe est protégé par l'algorithme CRYPT. Il s'agit ici de la méthode native de CRYPT qui est dérivée de l'algorithme DES. A ne pas confondre avec le CRYPT UNIX qui permet l'utilisation de divers algorithmes en fonction de l'OS.

La méthode de hash la plus sécurisée est SSHA. Nous vous en recommandons l'utilisation. La méthode SRP stocke également des informations pour authentifier les utilisateurs, mais ces informations sont sous la forme d'une clé Diffie-Hellman et d'une graine aléatoire. Ces deux informations sont stockées dans des champs du schéma LDAP NETASQ.

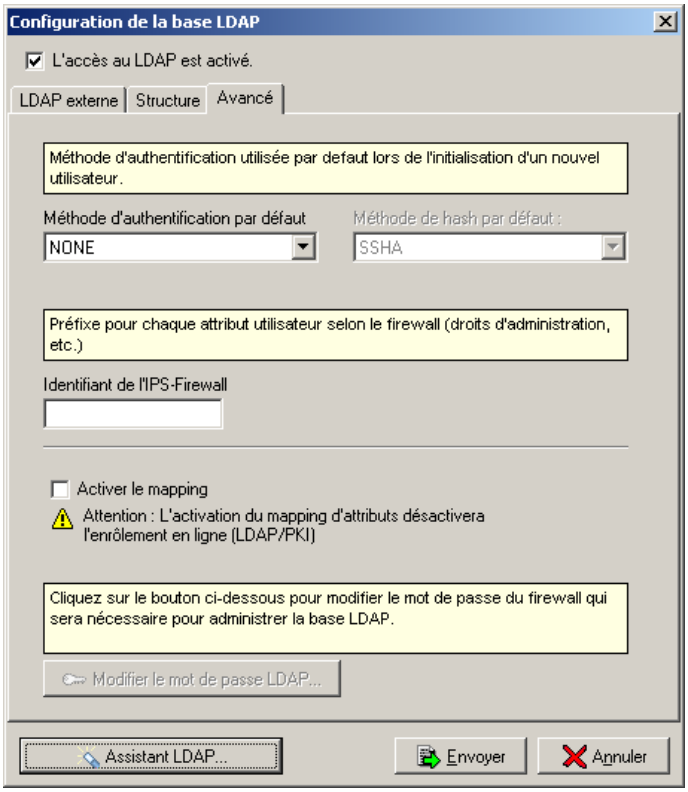
Identifiant de l'IPS-Firewall

Tous les utilisateurs de la base LDAP sont préfixés du numéro de série de l'IPS-Firewall sur lequel la base LDAP a été créée (préfixe par défaut). Mais lorsque l'IPS-Firewall est remplacé ou lorsque la configuration de la base LDAP est sauvegardée puis restaurée sur un autre IPS-Firewall, le préfixe par défaut n'est alors plus valide. Cette option permet de spécifier un préfixe non attaché à l'IPS-Firewall.

Modifier le mot de passe LDAP

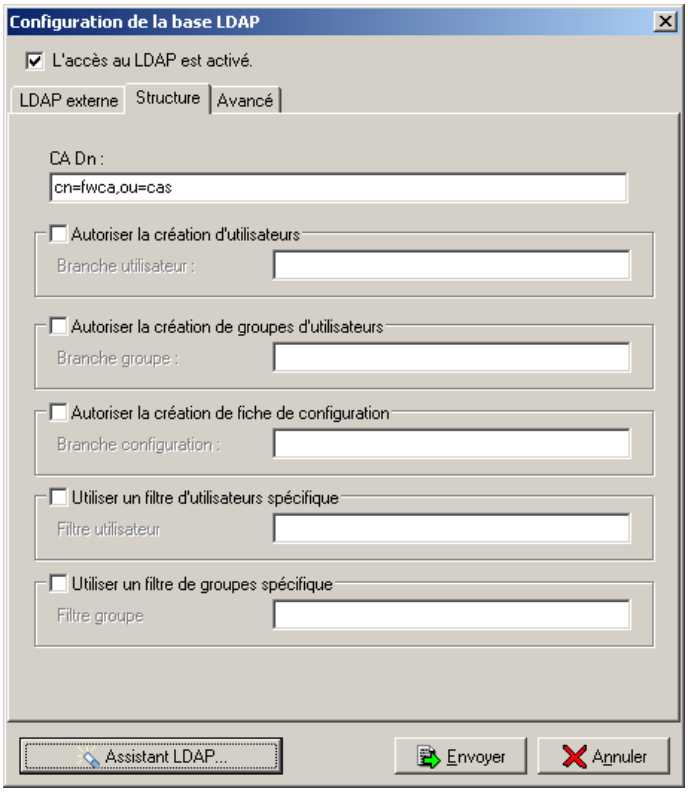
Cette option permet de modifier le mot de passe de configuration de la base LDAP.

Onglet Avancé (LDAP externe ou Active Directory)


Configuration de la base LDAP
L'accès au LDAP est activé.
LDAP externe
Structure
Avancé
Méthode d'authentification utilisée par defaut lors de l'initialisation d'un nouvel utilisateur.
Méthode d'authentification par défaut
NONE
Méthode de hash par défaut :
SSHA
Préfixe pour chaque attribut utilisateur selon le firewall (droits d'administration, etc.)
Identifiant de l'IPS-Firewall
Activer le mapping
Attention : L'activation du mapping d'attributs désactivera l'enrôlement en ligne (LDAP/PKI)
Cliquez sur le bouton ci-dessous pour modifier le mot de passe du firewall qui sera nécessaire pour administrer la base LDAP.
Modifier le mot de passe LDAP...
Assistant LDAP...
Envoyer
Annuler

L'onglet Avancé pour une configuration de base externe possède une option supplémentaire : « Activer le mapping ». Cette option permet d'activer le mapping (correspondance) entre les objets du schéma LDAP NETASQ, utilisés par le firewall, et les objets d'un autre annuaire. Lorsque cette option est cochée, un nouvel onglet (onglet Mapping) apparaît.

Onglet Structure



Cet onglet est ajouté lorsqu'une base LDAP externe ou Active Directory est utilisée.

Les options de cet onglet vous permettent d'ajouter, dans la base LDAP externe ou Active Directory, les fiches utilisateurs créées dans la configuration des objets. Les utilisateurs et les groupes seront chacun stockés dans une branche spécifique de l'annuaire LDAP ou Active Directory.

CA DN

Ce champ définit l'emplacement de l'autorité de certification présente dans la base LDAP externe ou Active Directory. Cet emplacement est notamment utilisé lors de la recherche de la CA utilisé pour la méthode d'authentification SSL. Il n'est pas indispensable de configurer ce champ mais dans ce cas, pour que la méthode d'authentification SSL fonctionne, il faut spécifier la CA dans la liste des CA de confiance dans la configuration de la méthode SSL (Voir « Méthode d'authentification SSL »).

Autoriser la création d'utilisateurs

Donnez le nom de la branche LDAP pour stocker les utilisateurs. Exemple : ou=users.

Autoriser la création de groupes d'utilisateurs

Donnez le nom de la branche LDAP pour stocker les groupes d'utilisateurs. Exemple : ou=groups.

Autoriser la création de fiche de configuration

Donnez le nom de la branche LDAP pour stocker les configurations. Exemple : ou=configuration.

Utiliser un filtre d'utilisateurs spécifique

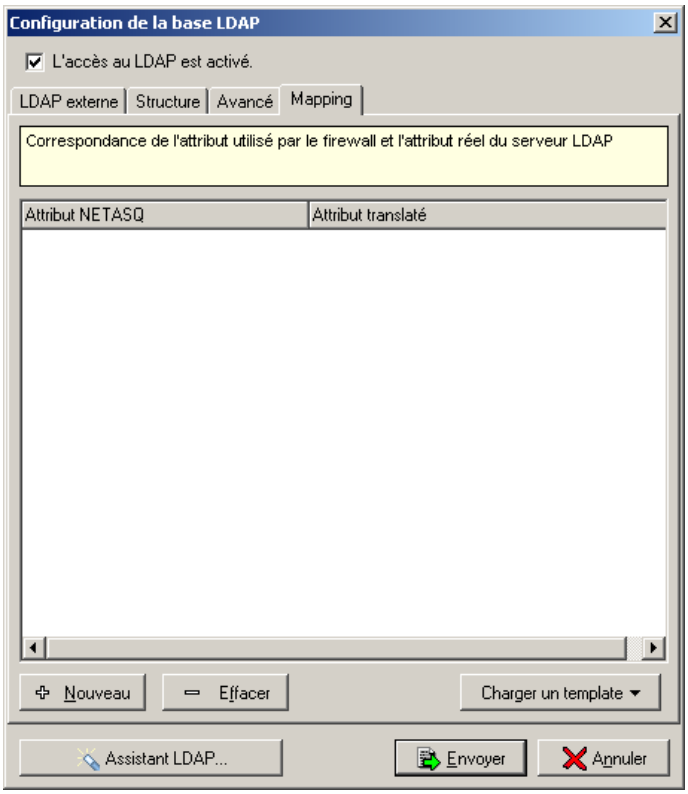
Lors de l'utilisation de l'IPS-Firewall en interaction avec une base externe, seuls les utilisateurs correspondants au filtre seront utilisés. Par défaut ce filtre correspond à ObjectClass = InetOrgPerson.

© Copyright NETASQ 2006

Utiliser un filtre de groupes spécifiques

Lors de l'utilisation de l'IPS-Firewall en interaction avec une base externe, seuls les utilisateurs correspondants au filtre seront utilisés. Par défaut ce filtre correspond à ObjectClass = GroupOfNames.

Onglet Mapping



Cet onglet est ajouté lorsqu'une base LDAP externe ou Active Directory est utilisée et que l'option « Activer le mapping » de l'onglet Avancé est cochée (par défaut).

Les options de cet onglet vous permettent d'indiquer la correspondance entre les attributs utilisés par NETASQ et ceux utilisés dans la base externe.

Par exemple : le NETASQ attribute <uid> = l'Active Directory attribute <sAMAccountName>

Vous pouvez ajouter ou supprimer des correspondances d'attributs grâce aux boutons « Nouveau » et « Effacer ».

Charger un template

Ce bouton vous permet de spécifier une liste de correspondance, déjà définie par NETASQ, avec des produits du marché (Active Directory, OpenDirectory…).

Qu'est-ce que c'est ?

La PKI ou Public Key Infrastructure (infrastructure à clé publique) est un système cryptographique (basé sur la cryptographie asymétrique). Elle utilise des mécanismes de signature et certifie des clés publiques (en associant une clé à un utilisateur) qui permettent de chiffrer et de signer des messages ainsi que des flux de données, afin d'assurer confidentialité, authentification, intégrité et non-répudiation.

Ces quatre notions (confidentialité, authentification, intégrité et non-répudiation) sont les bases de toutes solutions de sécurité. Toutefois, elles ne sont pas développées dans la suite de ce document. Si vous sentez le besoin d'approfondir vos connaissances sur ces concepts, un ouvrage générique sur la sécurité vous apportera les bases nécessaires à leur compréhension.

Principe

La PKI est un système basé sur une autorité de confiance (votre firewall NETASQ par exemple) qui signe et délivre des certificats contenant une bi-clé associée à des informations propriétaires à un utilisateur.

Ces certificats sont de véritables passeports électroniques qui servent à l'authentification des utilisateurs. De plus, ils contiennent les clés de chiffrement et déchiffrement qui garantissent la confidentialité des données.

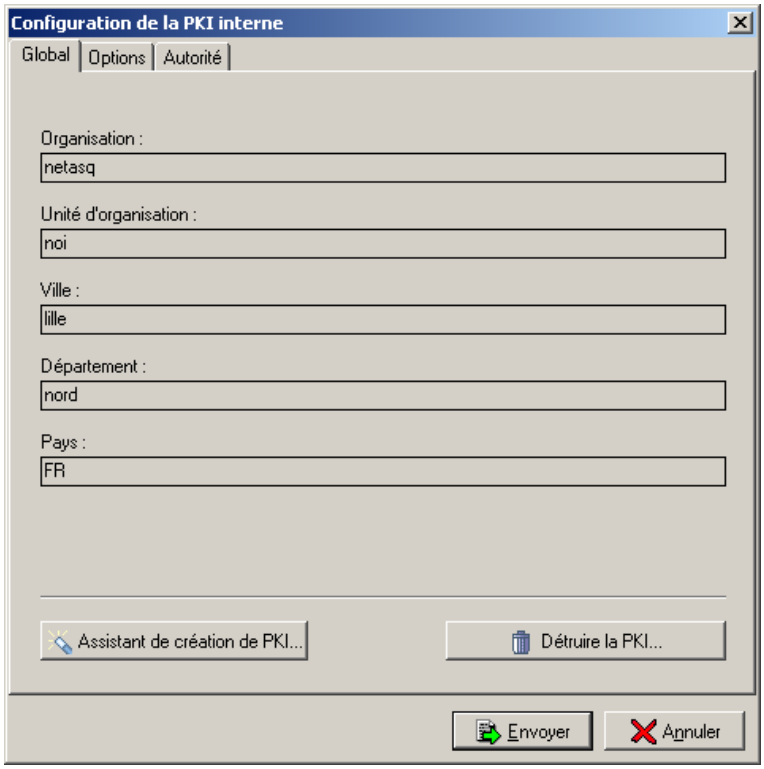
Intérêt de la PKI

Une infrastructure à clé publique est une couche de sécurité supplémentaire par rapport à un système d'authentification « simplement » basé sur un annuaire LDAP. La bi-clé, le certificat, l'autorité de confiance sont utilisés pour sécuriser les échanges sur l'Internet.

Le certificat est une alternative « sympathique » aux systèmes de log on car l'utilisateur n'a plus à retenir de mot de passe. En effet la portabilité du certificat lui permet d'être intégré dans des solutions du type clé USB par exemple.

De la même façon le certificat peut être utilisé pour les tunnels VPN. Il n'est plus nécessaire de partager un secret qu'il est difficile de s'échanger à l'abri des regards indiscrets du monde du web.

© Copyright NETASQ 2006



Les IPS-Firewalls NETASQ possèdent une PKI interne (sauf le modèle F50), vous permettant de créer des certificats numériques pour vos utilisateurs. Ces certificats peuvent être utilisés pour l'authentification des utilisateurs au travers du firewall, pour l'authentification VPN. Ils peuvent aussi être utilisés par des applications de votre système d'information.

Cette fenêtre est accessible par le sous-menu « PKI > Général ». Elle vous permet de visualiser et de configurer votre PKI après l'avoir initialisée.

Elle se décompose en deux parties :

► une zone d'onglets et la fenêtre correspondant à l'onglet choisi. Les onglets disponibles vous permettent respectivement de visualiser les informations de votre configuration, de modifier certaines options, de visualiser les informations de votre PKI,

► une zone en bas à droite avec deux boutons vous permettant d'envoyer vos modifications au Firewall ou de quitter cette fenêtre sans prendre en compte les modifications.

Si vous accédez à cette section pour la première fois, vous devrez configurer la PKI en utilisant l'assistant PKI.

Assistant PKI

Cet assistant se lance automatiquement lors du premier accès au sous-menu « PKI > configuration » ou lorsque vous cliquez sur le bouton « Assistant de création de PKI » sur l'écran de configuration générale.

Etape 1

© Copyright NETASQ 2006

Lors de cette première étape, vous devez renseigner les informations générales concernant la PKI que vous voulez mettre en oeuvre. Les informations saisies se retrouveront dans le certificat de votre autorité de certification et dans les certificats de vos utilisateurs.

Organisation	Nom de votre société (ex : NETASQ).
Unité d'Organisation	"branche" de votre société (ex : INTERNE).
Localité	Ville de votre société (ex : Villeneuve d'Ascq).
Département	Département géographique de votre société (ex : Nord).
Pays	Choisissez dans la liste le pays de la société (ex : France)

Etape 2

Dans cette seconde étape du wizard de configuration de la PKI, vous devez renseigner un mot de passe qui va permettre la protection de la clé privée de votre autorité de certification. Ce mot de passe est très important, si vous le perdez, il vous sera impossible par la suite de générer des certificats utilisateurs, de générer des CRLs, ...

Remarque : le choix d'un mot de passe trop simple est déconseillé. Nous vous recommandons de mélanger les lettres minuscules, majuscules, les chiffres, les caractères spéciaux.

Etape 3

Dans la troisième étape du wizard de configuration de la PKI, vous devez renseigner la configuration concernant le matériel cryptographique de votre PKI.

Cette étape est décomposée en deux :

- ► Configuration du matériel cryptographique pour l'autorité de certification,
- ► Configuration du matériel cryptographique pour les utilisateurs.

Matériel cryptographique pour l'autorité de certification :

Taille de clé : taille de la clé de votre autorité exprimée en bits. Cette valeur ne sera pas modifiable par la suite. Plus la taille est grande, plus la sécurité est importante.

Validité du Certificat : le nombre de jours durant lesquels votre certificat d'autorité et par conséquent votre PKI seront valide. Cette date influe sur tous les aspects de votre PKI, en effet, une fois ce certificat expiré, tous les certificats utilisateurs le seront également. Cette valeur ne sera pas modifiable par la suite.

Validité de la liste de révocation : le nombre de jours durant lesquels votre CRL sera valide.

Il est normal de mettre à jour régulièrement votre CRL et donc de ne pas mettre une date trop importante pour la validité de votre CRL. Cette valeur sera modifiable par la suite.

Matériel cryptographique pour les utilisateurs :

Taille de clé : taille de la clé pour vos utilisateurs exprimée en bits. Cette valeur sera modifiable par la suite.

Validité du Certificat : le nombre de jours durant lesquels les certificats utilisateurs seront valides. Cette valeur sera modifiable par la suite.

Numéro de série pour le premier certificat

Cette fonctionnalité permet de définir manuellement ou de façon aléatoire le premier numéro de certificat généré par la PKI. Ainsi le nombre de certificats générés par la PKI est invisible à une tierce personne. Par exemple si le premier numéro est 10245 et que l'administrateur génère 15 certificats, le quinzième certificat porte donc le numéro 10259 et il est impossible de savoir s'il y a eu 10259 certificats effectivement générés.

Le champ « Nombre hexadécimal 64 bits » permet de spécifier le numéro du premier certificat généré sous la forme d'un nombre hexadécimal de 64 bits. Le bouton représentant un dé génère ce nombre de façon aléatoire.

Etape 4

Dans cetteétape de l'assistant de configuration de la PKI, vous devez renseigner la configuration concernant la distribution de la CRL. Cette information sera intégrée aux certificats générés et permettra aux applications utilisant le certificat de récupérer automatiquement la CRL afin de vérifier la validité du certificat.

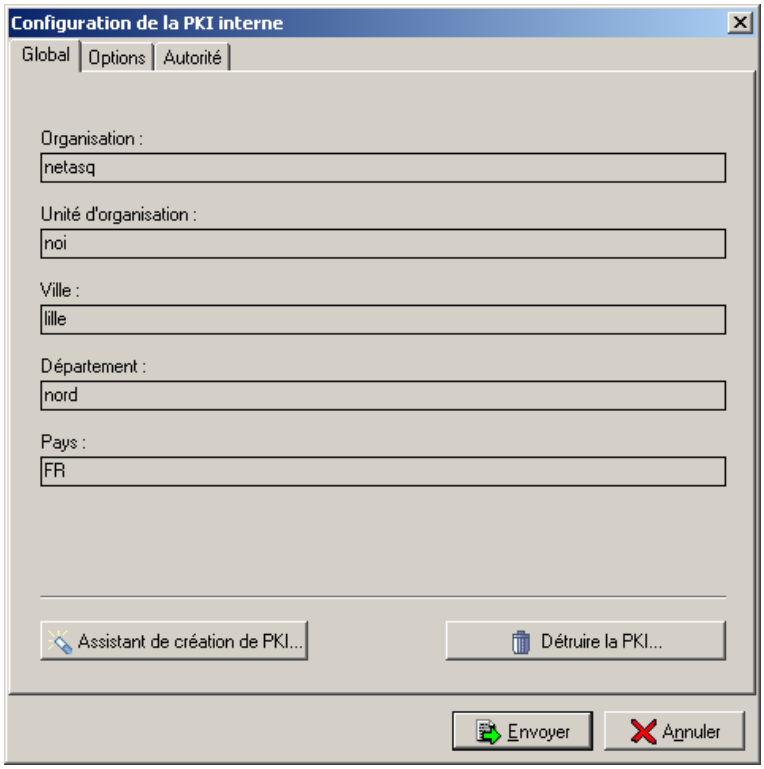
Dans le cas de l'utilisation de la PKI interne, il est fortement recommandé d'exporter la CA et la CRL NETASQ sur un serveur WEB (voir onglet Autorité) et de spécifier ici l'URL de ces deux fichiers stockés sur le serveur WEB. Cette opération doit être réalisée régulièrement afin que la CRL à disposition sur le serveur WEB soit la plus à jour possible. Une fois les champs « Protocole » et « URL » renseignés, il faut cliquer sur le bouton « Ajouter » pour créer le point de distribution.

Protocole	Protocole utilisé pour la diffusion de la CRL.
URL	Adresse du lieu de distribution de la CRL.
Liste des points de distribution	Liste de tous les points de distribution configurés avec les deux champs précédents.

Etape 5

Dans cette dernière étape de la configuration de la PKI NETASQ, il s'agit de spécifier si l'enrôlement des utilisateurs est autorisé en sélectionnant l'option « Autoriser l'enrôlement des utilisateurs ».

Onglet Global



Cet onglet est décomposé en trois parties :

► une zone informative sur la configuration actuelle de la PKI. Les informations affichées sont celles renseignées durant la première étape du Wizard d'initialisation de la PKI,

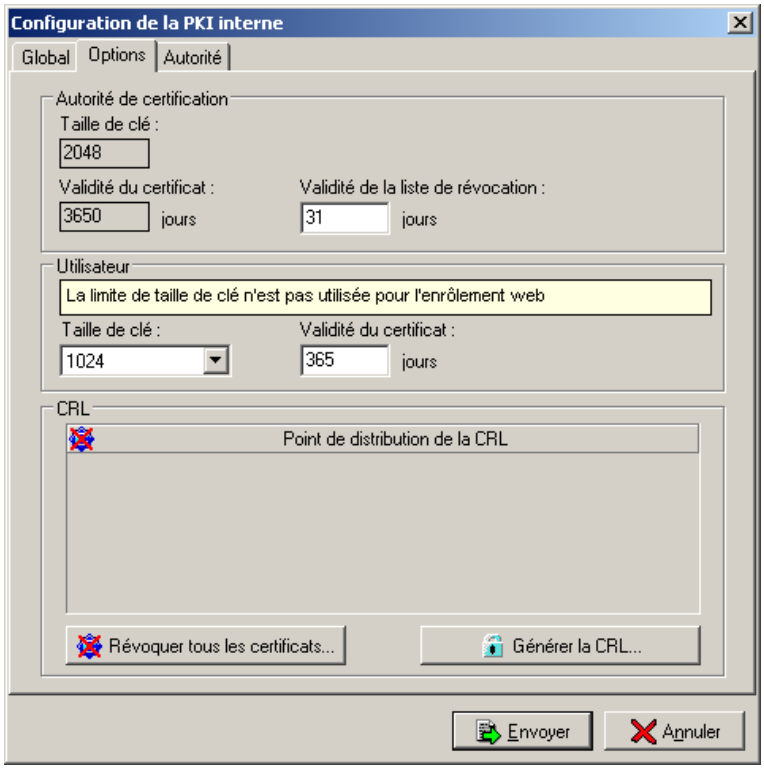
► une zone contenant deux boutons permettant :

► d'initialiser une nouvelle PKI (détruit la PKI actuelle),
► de détruire la PKI actuelle.

► une zone en bas à droite avec deux boutons vous permettant d'envoyer vos modifications au Firewall ou de quitter cette fenêtre sans prendre en compte les modifications.

Attention, le compte « admin » vous permet de détruire une PKI sans indiquer le mot de passe de l'autorité de certification. Cette fonctionnalité permet à l'administrateur de détruire une PKI même s'il oublie ce mot de passe.

Onglet Options



Cet onglet est décomposé en quatre parties :

► une zone informative sur la configuration du matériel cryptographique pour l'autorité de certification. Les informations affichées sont celles renseignées durant la seconde étape du Wizard d'initialisation de la PKI. La validité de la CRL peut être modifiée,

► une zone informative sur la configuration du matériel cryptographique pour les utilisateurs. Les informations affichées sont celles renseignées durant la seconde étape du Wizard d'initialisation de la PKI. Les champs de cette zone peuvent être modifiés,

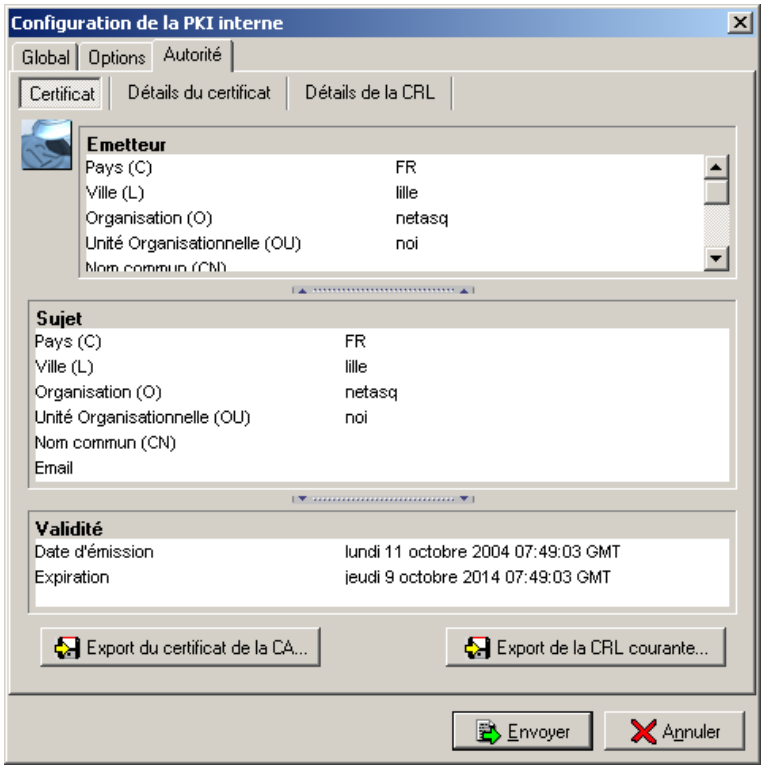
► une zone informative sur les points de distribution de CRL,

► une zone contenant deux boutons permettant :

► de révoquer tous les certificats utilisateurs. Dans ce cas, les certificats utilisateurs deviennent inutilisables,
► de générer une nouvelle CRL.

► une zone en bas à droite avec deux boutons vous permettant d'envoyer vos modifications au Firewall ou de quitter cette fenêtre sans prendre en compte les modifications.

Onglet Autorité



Cet onglet est décomposé en trois parties :

► une zone contenant trois onglets permettant d'obtenir :

► Une vision générale du contenu du certificat (Onglet Certificat),
► Le contenu complet du certificat (Onglet Détails du certificat),
► Le contenu complet de la CRL (Onglet Détails de la CRL). Vous pouvez voir les certificats qui ont été révoqués.

► une zone contenant deux boutons permettant :

► d'exporter le certificat de l'autorité de certification au format DER,
► d'exporter la CRL de l'autorité de certification au format .CRL.

► une zone en bas à droite avec deux boutons vous permettant d'envoyer vos modifications au Firewall ou de quitter cette fenêtre sans prendre en compte les modifications.

Lorsque l'authentification est activée, l'utilisateur doit passer par une phase de reconnaissance avant de pouvoir tenter une connexion au travers de l'IPS-Firewall. Deux cas peuvent se présenter :

Le filtrage d'URL est activé sur l'IPS-Firewall

Lorsque le filtrage d'URL et l'authentification sont activés au niveau de l'IPS-Firewall, l'utilisateur n'a pas besoin de se connecter à l'IPS-Firewall pour s'authentifier. La page d'authentification lui sera automatiquement envoyée lorsqu'il voudra se connecter à un site WEB. L'utilisateur sera alors authentifié pour tous les services auquel il est autorisé et pendant toute la période d'authentification.

Le filtrage d'URL n'est pas activé au niveau de l'IPS-Firewall

Dans ce cas, l'utilisateur doit s'authentifier sur l'IPS-Firewall avant de tenter une connexion nécessitant l'authentification. L'utilisateur doit se connecter au firewall via son navigateur internet, l'URL à utiliser est la suivante : https://<adresse IP du firewall>.
Exemple : https://10.0.0.254.

Missions de l'administrateur

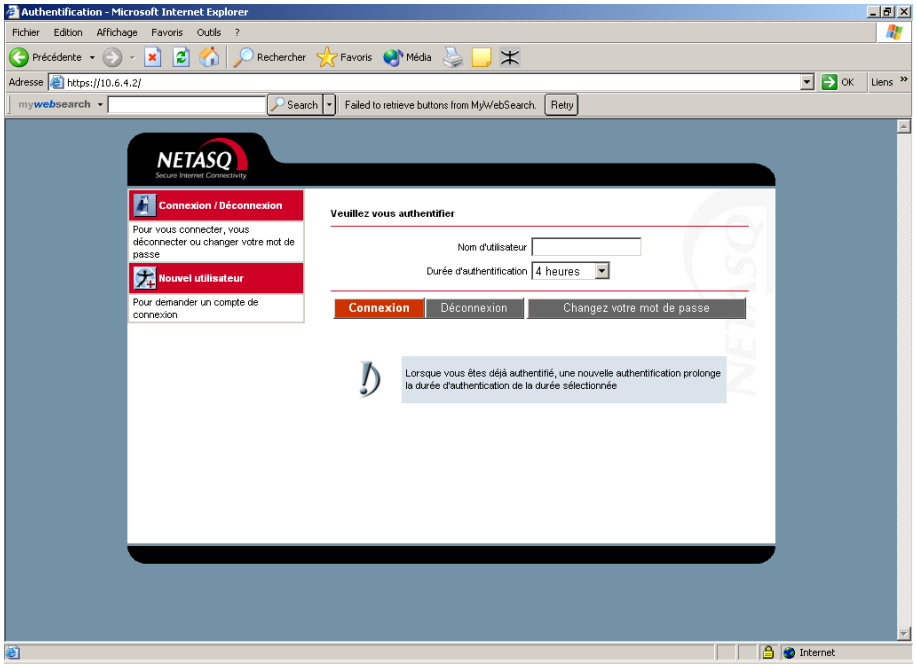
L'administrateur est le garant du bon usage des fonctionnalités d'authentification offertes par les équipements de son réseau et en particulier par son IPS-Firewall NETASQ. Dans ce cadre, NETASQ rappelle que la sensibilisation des utilisateurs à l'utilisation des pages d'authentification permet d'éviter leur mauvais usage.

Cette sensibilisation comprend :

► une aide à la définition de mots de passe ayant une entropie élevée (voir section « Sensibilisation des utilisateurs »),
► une formation à l'utilisation des fonctionnalités des pages d'authentification,
► une sensibilisation aux enjeux de la sécurité des ressources, des biens et des personnes.

Login

© Copyright NETASQ 2006


Authentification - Microsoft Internet Explorer
Fichier Edition Affichage Favoris Outils ?
Précédente Rechercher Favoris Média
Adresse https://10.6.4.2/
OK Liens
mywebsearch Search Failed to retrieve buttons from MyWebSearch. Retry
NETASQ
Secure Internet Connectivity
Connexion / Déconnexion
Pour vous connecter, vous déconnecter ou changer votre mot de passe
Nouvel utilisateur
Pour demander un compte de connexion
Veuillez vous authentifier
Nom d'utilisateur
Durée d'authentification 4 heures
Connexion
Déconnexion
Changez votre mot de passe
Lorsque vous êtes déjà authentifié, une nouvelle authentification prolonge la durée d'authentication de la durée sélectionnée
Internet

Dans les deux cas, pour s'authentifier, l'utilisateur doit saisir son login et la durée pendant laquelle il souhaite être authentifié, puis cliquer sur « Connexion ». Lorsque cette période est écoulée, l'utilisateur doit se ré-authentifier.

Attention, à ne pas mettre une durée trop longue pour des raisons de sécurité (l'utilisateur pourrait quitter son poste de travail sans le verrouiller et se faire intercepter sa session).

Selon la méthode choisie pour l'utilisateur, ce dernier doit ensuite, soit saisir son mot de passe, soit choisir un certificat numérique.

► Pour la méthode LDAP : saisie du mot de passe,
► Pour la méthode certificat (SSL) : choix d'un certificat (ce certificat doit au préalable avoir été installé sur le poste de l'utilisateur),
► Pour la méthode SRP : saisie du mot de passe (une applet Java est lancée et apparaît dans une nouvelle fenêtre pour l'utilisation de SRP).

L'utilisation de SRP implique l'installation d'une JVM (Java Virtual Machine) sur le poste utilisateur (la plupart des navigateurs WEB intègrent cette machine virtuelle). La JVM de SUN (version 1.4) est fortement conseillée.

Logout

Pour se déloger, il faut se connecter au firewall en https (voir précédemment), saisir le login de l'utilisateur désirant se déloger puis cliquer sur le bouton « Déconnexion ». L'utilisateur doit à nouveau saisir son mot de passe pour être délogé (évite qu'un utilisateur ne s'amuse à déloger d'autres utilisateurs).

Lorsqu'un utilisateur quitte son poste de travail avant la fin de la période d'authentification, il faut qu'il fasse un logout pour ne pas se faire intercepter sa session d'authentification.

Changement du mot de passe

L'utilisateur peut modifier son mot de passe d'authentification à distance. Pour cela, il suffit de saisir le login et de cliquer sur « Changez votre mot de passe ».

L'utilisateur n'a plus qu'à modifier son mot de passe.

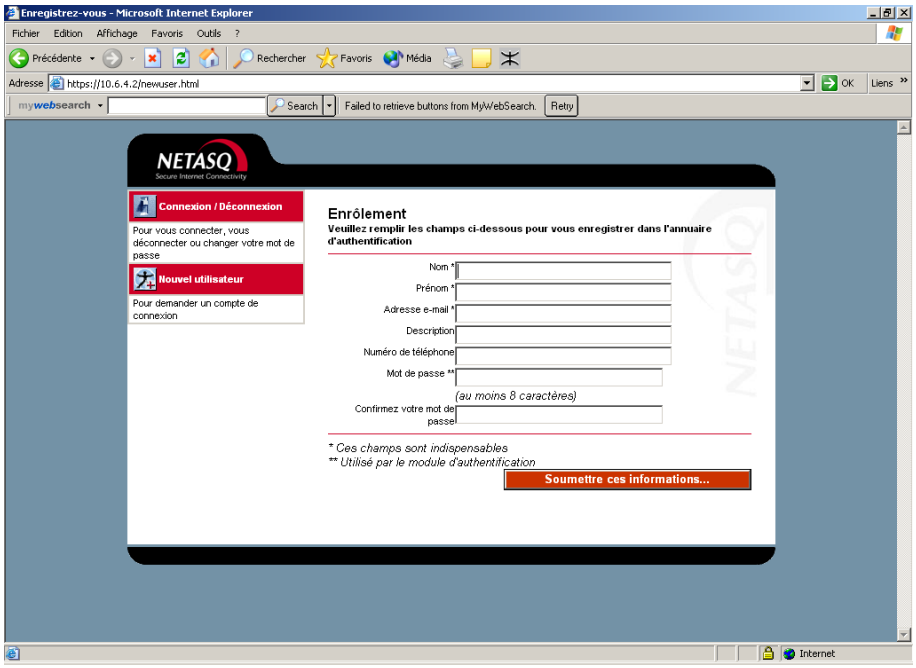
Remarque : Le changement de mot de passe ne fonctionne pas pour l'authentification en SSL avec certificats ou pour une authentification avec un serveur RADIUS externe.

Lorsqu'un service d'authentification est mis en place, il faut définir chaque utilisateur autorisé en créant un objet « utilisateur » (cf. configuration des objets). Plus la société est importante plus cette tâche est fastidieuse. Le service d'enrôlement WEB de NETASQ permet de faciliter cette tâche. Désormais c'est l'utilisateur « inconnu » qui demande la création de son compte et de son certificat (si une PKI a été définie par l'administrateur).

Requêtes des utilisateurs

Lorsque l'administrateur a spécifié dans la configuration générale de l'authentification, l'option « Autoriser l'enrôlement via le web » (Voir la « configuration de l'authentification »), le service d'enrôlement est activé. Le portail d'authentification web comporte désormais un bouton « Nouvel utilisateur » en plus.

En sélectionnant le bouton « Nouvel utilisateur », l'utilisateur accède au menu d'enrôlement et peut alors émettre sa requête d'enrôlement.


Enregistrez-vous - Microsoft Internet Explorer
Fichier Edition Affichage Favoris Outils ?
Précédente Rechercher Favoris Média
Adresse https://10.6.4.2/newuser.html
OK Liens
mywebsearch Search Failed to retrieve buttons from MyWebSearch. Retry
NETASQ
Secure Internet Connectivity
Connexion / Déconnexion
Pour vous connecter, vous déconnecter ou changer votre mot de passe
Nouvel utilisateur
Pour demander un compte de connexion
Enrôlement
Veuillez remplir les champs ci-dessous pour vous enregistrer dans l'annuaire d'authentification
Nom *
Prénom *
Adresse e-mail *
Description
Numéro de téléphone
Mot de passe **
(au moins 8 caractères)
Confirmez votre mot de passe
* Ces champs sont indispensables
** Utilisé par le module d'authentification
Soumettre ces informations...
Internet

Suivant la méthode d'enrôlement (LDAP ou LDAP et PKI), différents champs sont à remplir :

Last Name	Nom de l'utilisateur (ce champ est obligatoire).
First Name	Prénom de l'utilisateur (ce champ est obligatoire).
Email Adress	Adresse électronique (ce champ est obligatoire).
Description	Description succincte concernant l'utilisateur.
Phone Number	Champ réservé au téléphone.

© Copyright NETASQ 2006

Passphrase	Mot de passe utilisateur utilisé pour l'authentification.
Confirm passphrase	Confirmation du mot de passe.
Cryptographic Service Providers	Taille de la clef privée de l'utilisateur (uniquement dans le cas d'un enrôlement LDAP et PKI).

Gestion des requêtes

Lorsqu'un utilisateur a envoyé une requête, l'administrateur peut gérer ces requêtes en attente. Deux menus sont utilisés pour la gestion des requêtes :

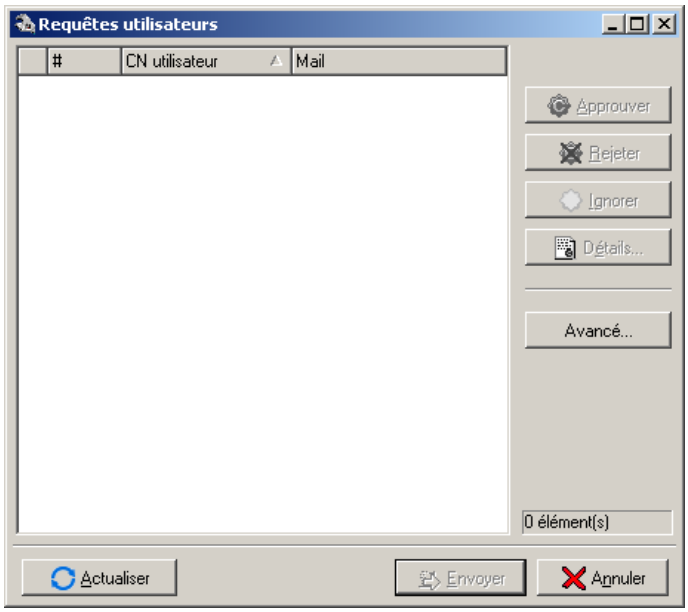
► Liste des requêtes utilisateurs : gestion des requêtes de création des comptes utilisateurs, cette liste est accessible par le menu « Authentification > Liste des requêtes d'utilisateurs »,

► Liste des requêtes de certificats : gestion des requêtes de création de certificats, cette liste est accessible par le menu « PKI > Liste des requêtes de certificats ».

Les options de configurations de ces deux menus sont relativement identiques.

Validation et rejet des requêtes

Lorsque vous accédez au menu « Liste des requêtes d'utilisateurs » (ou au menu Liste des requêtes de certificats », l'écran de gestion des requêtes s'affiche.



Cet écran se divise en deux :

► A gauche : la liste des requêtes en attente,
► A droite : les actions réalisables.

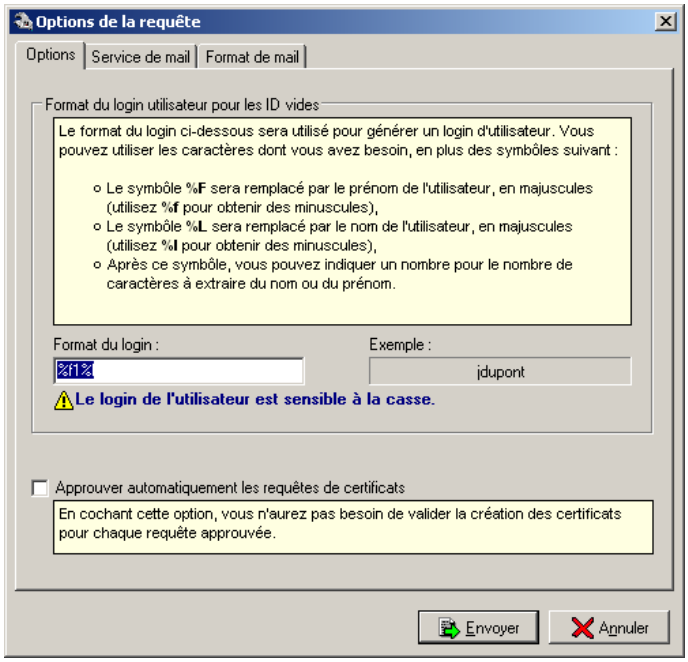
Approuver	Ce bouton vous permet d'approuver la requête de l'utilisateur.
Rejeter	Ce bouton vous permet de rejeter la requête de l'utilisateur.
Ignorer	Ce bouton vous permet d'ignorer la requête de l'utilisateur.

Détails	Ce bouton vous permet d'accéder à une visualisation des détails de la requête de l'utilisateur.
Avancé	Ce bouton vous permet d'accéder aux options de l'enrôlement WEB.

Toute action de cet écran n'est validée que lorsque vous appuyez sur le bouton « envoyer ». Si vous validez (ou rejetez) par mégarde une requête vous pouvez utiliser le bouton « ignorer » pour remettre en attente la requête d'un utilisateur.

Options des requêtes

Appuyer sur le bouton « Avancé » du menu menu « Liste des requêtes d'utilisateurs » (ou au menu Liste des requêtes de certificats ») vous permet d'accéder au menu de configuration des options des requêtes. Cet écran se divise en trois onglets :


Options de la requête
Options
Service de mail
Format de mail
Format du login utilisateur pour les ID vides
Le format du login ci-dessous sera utilisé pour générer un login d'utilisateur. Vous pouvez utiliser les caractères dont vous avez besoin, en plus des symbôles suivant :
Le symbôle %F sera remplacé par le prénom de l'utilisateur, en majuscules (utilisez %f pour obtenir des minuscules),
Le symbôle %L sera remplacé par le nom de l'utilisateur, en majuscules (utilisez %l pour obtenir des minuscules),
Après ce symbôle, vous pouvez indiquer un nombre pour le nombre de caractères à extraire du nom ou du prénom.
Format du login :
%f1%
Exemple :
jdupont
Le login de l'utilisateur est sensible à la casse.
Approuver automatiquement les requêtes de certificats
En cochant cette option, vous n'aurez pas besoin de valider la création des certificats pour chaque requête approuvée.
Envoyer
Annuler

► **Options** : configuration des options générales de l'enrôlement :

► Chaîne de format : la configuration de cette chaîne est explicitée dans l'application,

► « Approuver automatiquement les requêtes de certificats » : (uniquement pour le menu « Liste des requêtes d'utilisateurs ») cette option vous permet la validation automatique des requêtes de certificats. Lorsque l'administrateur valide la requête de création de compte utilisateur, l'application validera automatiquement la création du certificat associé à cet utilisateur.

► **Service de Mail** : activation de l'envoi automatique des réponses aux requêtes. Vous ne pouvez démarrer ce service que si vous avez au préalable activé l'envoi des notifications d'alarmes dans le menu ASQ. Cette option permet l'envoi d'un email à l'utilisateur pour lui préciser que sa requête a été validée ou non et qu'il peut s'authentifier ou retirer son certificat.

► **Format de Mail** : formatage des mails de validation et de rejet. Cet onglet n'est disponible que si le service de mail est activé. Il vous permet de définir un modèle de mail de validation ou de rejet de requête. Certaines de ces informations sont dynamiques (par exemple $LastName, dans le modèle par défaut, affiche le nom de l'utilisateur) :

► $LastName (Prénom de l'utilisateur),
► $FirstName (Nom de l'utilisateur),
► $Date (date de génération de la requête d'enrôlement),

© Copyright NETASQ 2006

► $URL (lien web pour récupération du certificat validé),
► $UID (login attribué par l'administrateur).

Lorsque la requête de l'utilisateur est validée par l'administrateur. Il peut désormais s'authentifier sur le firewall pour bénéficier des services auxquels il a accès. Il est mis au courant de cette validation par mail, si le service de mail a été activé.

Lorsque la requête de création d'un certificat est validée l'utilisateur peut retirer ce certificat :

► soit par défaut sur le firewall, à l'adresse https:\\<adresse du firewall>, en cliquant sur le bouton « Certificats » de la page,

► soit à l'adresse spécifiée par l'administrateur sur un poste externe au firewall.

L'administrateur de l'IPS-Firewall est responsable de la formation des utilisateurs quant à la sécurité du réseau, des équipements qui le composent et des informations qui y transitent.

En effet la plupart des utilisateurs d'un réseau sont néophytes en informatique et à fortiori en sécurité des réseaux. Il incombe donc à l'administrateur ou au responsable de la sécurité du réseau de mettre en place des sessions de formation ou tout du moins des campagnes de sensibilisation à la sécurité des réseaux.

Lors de ces sessions, il est important d'insister sur la gestion des mots de passe de l'utilisateur et de son environnement de travail et la gestion de leurs accès aux ressources de l'entreprise.

Gestion des mots de passe de l'utilisateur

Au cours de l'évolution des technologies de l'information, de nombreux mécanismes d'authentification ont été inventés et mis en place afin de garantir une meilleure sécurité des systèmes d'information des entreprises. Cette multiplication des mécanismes a entraîné une complexité qui contribue aujourd'hui à détériorer la sécurité des réseaux d'entreprises.

Les utilisateurs (néophytes et non formés) choisissent des mots de passe « simplistes », tirés généralement de leur vie courante et la plupart du temps correspondant à un mot contenu dans un dictionnaire. Ces comportements entraînent, bien entendu, une dégradation notable de sécurité du système d'information.

Il faut prendre conscience que l'attaque par dictionnaire est un « outil » plus que performant. Une étude de 1993 montre déjà cet état de fait. La référence de cette étude est la suivante : (http://www.klein.com/dvk/publications/). Ce qui est le plus frappant dans cette étude est sûrement le tableau présenté ci-dessous (basé sur un mot de passe de 8 caractères) :

Type de mot de passe	Nombre de caractères	Nombre de mots de passe	Tempsde Cracking
Lexique anglais 8 carac. et +	special	250000	< 1 seconde
casse minuscule uniquement	26	208827064576	9 heures
casse minuscule + 1 majuscule	26/special	1670616516608	3 jours
minuscules et majuscules	52	53459728531456	96 jours
Lettres + chiffres	62	218340105584896	1 an
Caractères imprimables	95	6634204312890620	30 ans
Jeu de caractères ASCII 7 bits	128	72057594037927900	350 ans

On peut citer aussi un état de fait qui tend à se résorber mais qui est encore d'actualité : les fameux post-its collés à l'arrière des claviers.

L'administrateur doit mettre en place des actions (formation, sensibilisation, …) dans le but de modifier et de corriger ses « habitudes ». Par exemple :

► Incitez vos utilisateurs à choisir des mots de passe de longueur supérieure à 7 caractères,
► Demandez-leur d'utiliser des chiffres et des majuscules,
► De changer souvent de mots de passe,

© Copyright NETASQ 2006

► Et surtout de ne noter en aucun cas le mot de passe qu'ils auront finalement choisi.

L'une des méthodes classiques pour trouver un bon mot de passe est de choisir une phrase que l'on connaît par cœur (vers d'une poésie, parole d'une chanson) et d'en tirer les premières lettres de chaque mot. Cette suite de caractères peut alors être utilisée comme mot de passe. Par exemple :

► « **N**ETASQ, **1**er **c**onstructeur **f**rançais **d**e **b**oîtiers **F**IREWALL **e**t **V**PN… »

Le mot de passe pourrait être le suivant : N1cfdbFeV.

Environnement de travail

L'espace de travail est souvent un lieu de passage, un croisement pour de nombreuses personnes internes et extérieures à l'entreprise. Il s'agit donc de sensibiliser les utilisateurs au fait que certaines personnes (fournisseurs, clients, ouvriers, …) peuvent accéder à leur espace de travail et de ce fait recueillir des informations sur l'activité de l'entreprise.

Il est important de faire prendre conscience à l'utilisateur qu'il ne faut pas qu'il divulgue son mot de passe aussi bien par téléphone que par Email (social engineering) et qu'il faut qu'il tape son mot de passe à l'abri des regards indiscrets.

Gestion des accès d'utilisateurs

Pour compléter ce chapitre sur la sensibilisation des utilisateurs à la sécurité des réseaux, l'administrateur doit aborder la gestion des accès utilisateur. En effet le mécanisme d'authentification d'un IPS-Firewall NETASQ (comme beaucoup d'autres systèmes) basé sur un système de login / mot de passe n'implique pas forcément de délogage à fermeture de l'application à l'origine de cette authentification (crédit de temps d'authentification). Cet état de fait n'est pas forcément évident pour l'utilisateur néophyte. Ainsi malgré avoir fermé l'application en question, l'utilisateur (qui pense ne plus être connecté) reste authentifié. S'il quitte son poste une personne mal-intentionnée peut alors usurper son identité et accéder aux informations contenues dans l'application.

Enfin incitez les utilisateurs à verrouiller leurs sessions lorsqu'ils se déplacent et laissent leur poste de travail sans surveillance. Cette tâche qui se révèle parfois fastidieuse peut être facilitée par des mécanismes d'authentification qui automatise le verrouillage (token USB par exemple).

Chapitre VIII

Haute disponibilité

© Copyright NETASQ 2006

Pour cette section, vous devez avoir franchi les étapes

► Installation, pré-installation, intégration.

Utilité de la section

Cette section vous permet de configurer le Watchdog, élément hardware qui teste régulièrement l'IPS-Firewall afin de détecter une éventuelle inactivité de celui-ci. Le Watchdog peut commander un reboot de l'IPS-Firewall en cas de freeze de ce dernier.

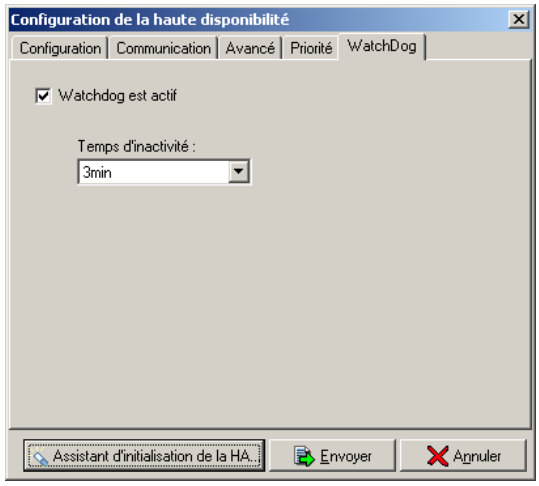
Accéder à cette section

Accédez à la boîte de dialogue par le sous-menu « IPS-Firewall > Haute Disponibilité ».

© Copyright NETASQ 2006

Important

Seuls les Firewalls sortis de production ou revenus en SAV depuis octobre 2001 peuvent avoir les fonctionnalités Watchdog et Haute Disponibilité. Si votre Firewall est plus ancien, vous pouvez également bénéficier de ces fonctionnalités. Dans ce cas, le Firewall devra néanmoins subir une modification matérielle, et donc revenir chez NETASQ pour intervention.



La fonctionnalité Watchdog va vous permettre d'automatiser le reboot du Firewall en cas de « gel ». Le principe est très simple : le Watchdog est un composant hardware qui réalise à intervalles réguliers des tests d'activité sur le Firewall. Au bout d'un certain temps (paramétrable) sans réponse, l'arrêt et le démarrage du Firewall ont lieu.

La configuration est très simple. Il suffit dans le menu Haute Disponibilité (onglet Firewall) de cocher « Watchdog est actif » et de déterminer le temps d'inactivité maximale. Les connexions actives sont récupérées après reboot.

Ne mettez pas une valeur de temps limite d'inactivité trop court (inférieur à 1 minute), vous risqueriez de faire rebooter le firewall fréquemment alors que ce n'est pas nécessaire. En effet, il peut arriver que le firewall ne répond plus durant quelques secondes et reprenne une activité normale aussitôt après, sans que cela ne nécessite un reboot.

Cette fonctionnalité est accessible indépendamment de la haute disponibilité.

© Copyright NETASQ 2006

Pour cette section, vous devez avoir franchi les étapes

► Installation, pré-configuration, intégration,
► Demande de clés d'activation pour la haute disponibilité auprès de NETASQ,

Pour cette section, vous devez connaître

► La politique de sécurité de l'entreprise,
► Le mot de passe de l'utilisateur « HA »,
► L'adresse IP du lien de gestion de la Haute Disponibilité.

Utilité de la section

Cette section vous permet de configurer la fonctionnalité de haute disponibilité. Cette fonctionnalité n'est utilisable que si vous avez deux IPS-Firewalls en votre possession.

Le principe sera de basculer toutes les connexions de l'IPS-Firewall actif vers le second (firewall passif) en cas de dysfonctionnement du firewall actif.

Accéder à cette section

Accédez à la boîte de dialogue par le sous-menu « IPS-Firewall > Haute Disponibilité ».

Vous devez être connecté avec les privilèges de modification pour pouvoir effectuer ces modifications et posséder deux IPS-Firewalls.

© Copyright NETASQ 2006

Pour utiliser la fonctionnalité de haute disponibilité, vous devez avoir deux IPS-Firewalls en votre possession.

Deux clés d'activation particulières doivent être demandées auprès de NETASQ (une pour chaque IPS-Firewall) et installées via l'interface graphique (Voir la section « Actions diverses > Licence »).

Notion de maître/esclave

Un des deux firewalls sera considéré comme maître et le second comme esclave (le statut de chaque firewall sera déterminé par la clé d'activation installée).

La différenciation maître et esclave sert dans les cas suivants :

► Si les deux firewalls démarrent simultanément,
► Si les deux firewalls se retrouvent dans le même état (suite à une perte de communication par l'interface Ethernet par exemple),
► Pour différencier les adresses IP affectées de chaque côté de la liaison haute disponibilité.

Seuls les Firewalls sortis de production ou revenus en SAV depuis octobre 2001 peuvent avoir les fonctionnalités Watchdog et Haute Disponibilité. Si votre Firewall est plus ancien, vous pouvez également bénéficier de ces fonctionnalités. Dans ce cas, le Firewall devra néanmoins subir une modification matérielle, et donc revenir chez NETASQ pour intervention.

© Copyright NETASQ 2006

Aucun élément réseau n'étant à l'abri d'une panne, la fonctionnalité de haute disponibilité (ou de tolérance de pannes) proposée sur les firewalls NETASQ permet d'assurer une continuité de service même en cas de dysfonctionnement.

Cette fonctionnalité nécessite l'utilisation de deux firewalls qui seront considérés par le réseau comme une seule entité. Ces deux firewalls possèdent la même configuration mais un seul firewall sera actif à un instant donné (un seul firewall prendra en charge les connexions). Le second firewall ne deviendra actif que lorsque le premier ne sera plus dans un mode de fonctionnement normal d'un firewall (les connexions actives sont récupérées lors du basculement).

Les interfaces réseau du firewall passif sont désactivées et ne sont réactivées automatiquement que lorsque le firewall redevient actif.

Les flux pour la haute disponibilité (tests d'activité, transfert des configurations ...) peuvent être acheminés via un câble ethernet. Il faut donc affecter une ou deux interfaces réseau sur chaque boîtier et relier ces deux interfaces via des liaisons ethernet. Vous pouvez soit dédier ces interfaces au fonctionnement de la Haute disponibilité ou soit réaliser la configuration de la haute disponibilité basée sur un VLAN.

La liaison Ethernet

NETASQ a choisi de ne plus supporter la haute disponibilité sur lien série car le débit sur un lien série n'était plus suffisant pour la base d'informations à répliquer entre les deux IPS-Firewalls. Dans le cas de la liaison Ethernet, le débit est beaucoup plus important, les transferts de configuration et la mise à jour de la base LDAP sont alors considérablement accélérés.

Remarque : avec la fonctionnalité de haute disponibilité, il est préférable d'utiliser une base externe afin d'éviter la réplication de la base LDAP interne entre les deux firewalls.

Il est possible de placer les deux boîtiers à des distances plus importantes l'un de l'autre.

Haute Disponibilité sur VLAN

La haute disponibilité sur VLAN permet d'utiliser la liaison Ethernet comme liaison de contrôle entre les deux IPS-Firewalls en haute disponibilité sans toutefois dédier cette interface. En effet grâce au support de la haute disponibilité sur VLAN, l'interface de contrôle peut alors être utilisé pour réaliser une DMZ par exemple.

Test de fonctionnement du firewall

Le firewall passif teste grâce à des pings (envoyés sur la liaison ethernet reliant les deux firewalls) si le firewall actif fonctionne. Ces tests sont réalisés de manière ponctuelle toutes les T secondes (T étant défini grâce au Firewall Manager, voir section "Mise en place"). Un bout d'un certain nombre de pings sans réponse (nombre paramétrable grâce au Firewall Manager), le firewall est considéré comme "freezé", c'est-à-dire ne répondant plus. Dans ce cas, le firewall passif devient actif et prend en charge les connexions.

En plus du ping, les firewalls se testent de manière croisée :

► Chacun demande de manière régulière l'état de l'autre (actif ou passif) pour détecter le cas où deux firewalls seraient actifs (cas où le câble série ou Ethernet dédié ont été débranchés). Dans ce cas, le firewall maître reste actif et l'esclave devient passif,

► Si le firewall actif a moins de cartes Ethernet en fonctionnement que le firewall passif (dysfonctionnement d'une carte), il sera basculé en mode passif alors que le passif deviendra actif,

© Copyright NETASQ 2006

► Si le firewall passif ne répond pas, une alarme du type "HA : défaillance du Firewall" sera envoyée.

► Si deux liaisons de contrôle ont été configurées, les firewalls vérifient d'abord leur connectivité par l'intermédiaire du premier lien de contrôle. Si cette liaison est rompue, la connectivité est testé sur le deuxième lien de contrôle avant qu'il y ait un basculement effectif.

Haute disponibilité sur deux liens de contrôle

La configuration de haute disponibilité NETASQ n'est viable que si à aucun moment, les deux appliances participant au cluster de haute disponibilité ne sont actifs simultanément. En effet dans le cas où les deux appliances serait actifs au même moment, cela poserait d'importants problèmes réseau car chaque appliance possède les mêmes adresses IP et les mêmes adresses MAC que son correspondant de haute disponibilité.

Pour parer à ce problème réseau, il est possible de configurer deux liens de contrôle. Ainsi si la connectivité entre les deux correspondants de haute disponibilité ne peut être établie sur le premier lien de contrôle (perte d'une interface, perte du lien…), elle est testée sur le deuxième lien de contrôle avant activation du firewall passif.

Spécificité de la deuxième liaison de contrôle

La première liaison de contrôle est chargée non seulement de la vérification de la connectivité entre les deux appliances participant à la haute disponibilité mais aussi de la synchronisation des informations entre l'appliance actif et l'appliance passif (synchronisation de la configuration, échange des tables de fonctionnement, etc). Tandis que le deuxième lien de contrôle permet uniquement la vérification de la connectivité entre les deux appliances. Elle permet donc d'empêcher un basculement inutile (passif vers actif) de l'appliance passif.

Avant de lire ce chapitre, vous devez avoir pris connaissance du chapitre « Licences » et avoir installé les deux clés d'activation.

Installation

Pour installer l'architecture de haute disponibilité, veuillez suivre la procédure suivante :

1. Les deux firewalls doivent être déconnectés du réseau local (dans le cas contraire, des problèmes de conflits d'adresses pourraient survenir) mais sous tension,

2. Connectez-vous au firewall esclave en changeant l'adresse IP du bridge (prenez par exemple l'adresse 10.0.0.253). Cette adresse doit absolument être différente de celle du firewall maître. Le firewall doit rebooter,

3. Reliez les deux firewalls avec un câble Ethernet,

4. Connectez-vous au firewall maître, Un assistant vous permet de configurer simplement la fonctionnalité de haute disponibilité. (bouton Assistant d'initialisation de la HA...).

Etape 1

Choisissez la ou les interfaces utilisées pour la haute disponibilité (pour le maître et pour l'esclave) et l'adresse IP du maître (l'adresse IP esclave = adresse IP maître +1). Si une interface VLAN est configurée, il est possible d'utiliser cette interface pour la haute disponibilité. Dans ce cas l'interface Ethernet à laquelle l'interface VLAN est rattachée n'est plus dédiée à la haute disponibilité.

Deuxième lien de contrôle

Notez qu'il est possible de configurer deux liens de contrôle grâce à l'assistant de configuration de la haute disponibilité. Ce deuxième lien de contrôle n'est utilisé que pour tester la connectivité existante entre les deux appliances participant au cluster de haute disponibilité.

Adressage des interfaces de haute disponibilité

Dans l'etape 1, vous définissez aussi le plan d'adressage utilisé par les interfaces des appliances participant aux liaisons de contrôle. L'assistant vous permet de définir l'adresse réseau et c'est lui-même qui attribue des adresses pour chacune des interfaces.

Notez qu'il est possible de définir à priori, n'importe quel plan d'adressage. Toutefois attention si vous définissez un plan d'adressage « public », l'accès aux sites WEB utilisant ce plan d'adressage sera impossible. Il est recommandé d'utiliser un plan d'adressage privé (différent de plus de celui utilisé par les autres interfaces).

Etape 2

Indiquez le temps entre deux pings dans le champ "intervalle" ainsi que le nombre de pings sans réponse accepté (seuil d'échec) avant un basculement du firewall actif vers le firewall passif.

Le seuil d'échec ne peut pas être inférieur à 2 et il est fortement déconseillé de mettre un intervalle de temps inférieur à 5 secondes.

© Copyright NETASQ 2006

Un intervalle de 15 secondes et un seuil d'échec de 2 sont conseillés.

La partie « Configuration du Watchdog » vous permet de définir le temps d'inactivité acceptable avant un reboot forcé de l'IPS-Firewall.

Etape 3

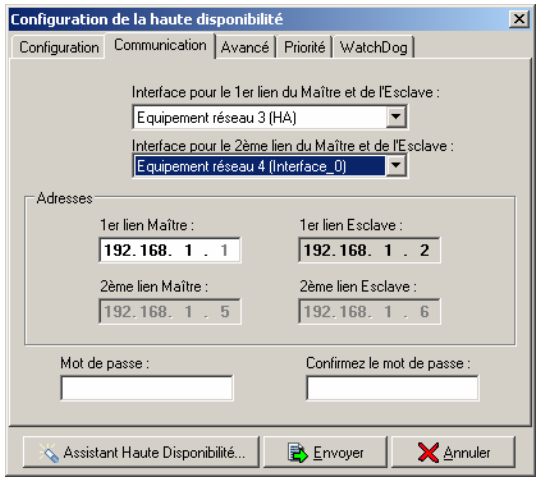
Enfin, indiquez le mot de passe utilisé pour chiffrer les communications entre les deux firewalls. Les firewalls communiquent entre eux sur le port 1300 et les données sont chiffrées en AES.

Tous les paramètres saisis dans cet assistant peuvent être modifiés par la suite.

5. Connectez-vous à l'autre firewall (firewall esclave) et relancez l'assistant. Attention, les interfaces, adresses IP et mots de passe doivent être identiques au firewall maître,

6. Une fois l'assistant réalisé sur les deux firewalls, vous devez vous connecter sur le MASTER (dans le cas où seul le SLAVE répond, faites une permutation manuelle) et faites une synchronisation des deux firewalls (voir plus bas). Il faut absolument que la première synchronisation soit faite du firewall MASTER vers le firewall SLAVE, pour une réplication des adresses MAC sur les deux boîtiers.

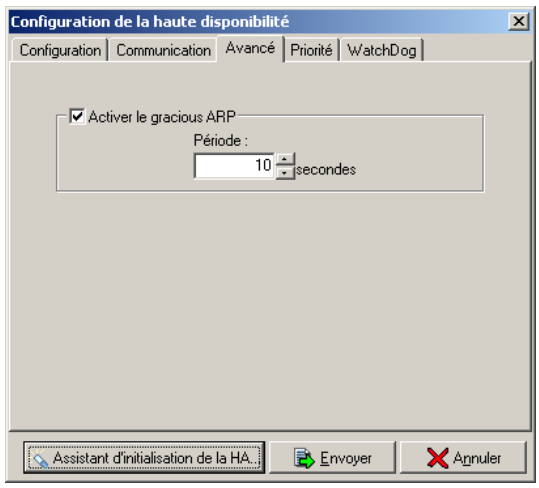
Onglet Communication



Dans ce menu vous pouvez modifier les paramètres définis dans l'assistant.

Interface pour le 1er lien du maître et de l'esclave	Interface principale utilisée pour relier les deux firewalls constituant le cluster.
Interface pour le 2ème lien du maître et de l'esclave	Interface secondaire utilisée pour relier les deux firewalls constituant le cluster.
Adresses	Adresses IP attribuées aux différents firewalls.
Mot de passe	Mot de passe utilisé pour chiffrer les communications entre les deux firewalls.

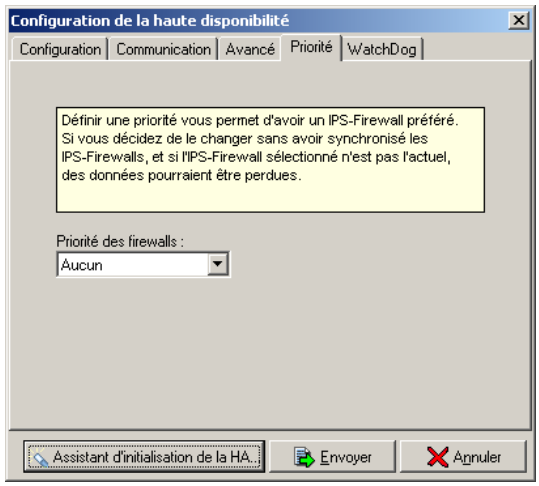
Onglet Avancé



Ce menu vous permet d'activer l'envoi de paquets du type « Gracious ARP ». C'est-à-dire que le firewall publie régulièrement, sur le réseau ,ses adresses IP et MAC.

Période	Intervalle de temps entre les différents envois de paquets.

Onglet Priorité



Dans le cas où les deux firewalls se retrouvent dans l'état actif ou démarrent en même temps, l'option priorité permet de spécifier quel firewall va prendre la main et quel firewall reprendra l'état passif.

Priorité des firewalls	Choix du firewall prioritaire.

Synchronisation des firewalls

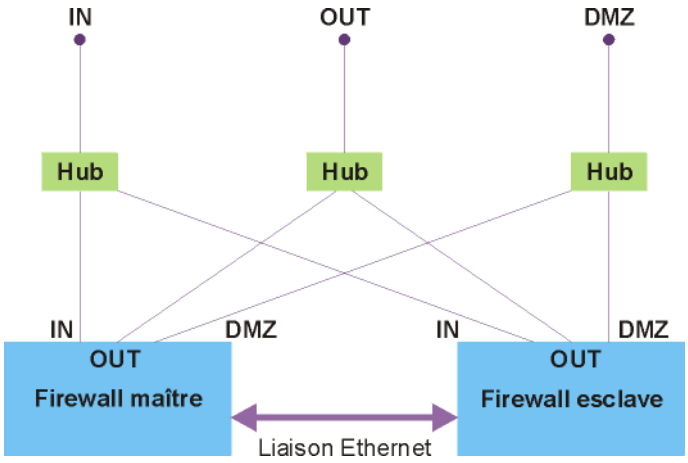
La synchronisation des firewalls permet la réplication de la configuration du firewall actif sur le firewall passif. Cette synchronisation est effectuée sur la configuration complète, les mots de passe, les changements de dates. La synchronisation peut être soit forcée en cliquant sur le bouton « Synchroniser » de l'onglet « Configuration », soit demandée par le Firewall Manager lorsqu'on quitte celui-ci.

Si vous faites une synchronisation manuelle, les firewalls seront indiqués comme non synchronisés, alors que la synchronisation a bien eu lieu. Pour vérifier la synchronisation, utilisez le moniteur temps réel qui vous donnera l'état de synchronisation des deux firewalls.

Permutation des firewalls

Si vous désirez rendre actif le firewall passif, cliquez sur le bouton « Permuter » de l'Onglet « Configuration ».

Schéma de mise en place de la Haute Disponibilité avec deux firewalls F500/4 et 3 Hubs 10/100Mbits de 4 ports avec les 3 interfaces des firewalls disponibles (la quatrième est utilisée pour la haute disponibilité).



Utiliser une liaison ethernet vous permet de séparer physiquement les deux boîtiers, en effet, vous pouvez placer chacun des firewalls dans une pièce différente. Par contre, vous perdez une interface Ethernet par boîtier (utilisées pour la haute disponibilité).

Remarque

L'utilisation de switchs à la place des hubs est possible mais fortement déconseillée, à cause du caractère "intelligent" de ces derniers. De plus, les hubs représentent un surcoût beaucoup moins important que les switchs.

© Copyright NETASQ 2006

Si vous désirez ne plus utiliser la fonctionnalité de haute disponibilité, veuillez suivre la procédure suivante :

1. Arrêter l'un des deux firewalls,

2. Arrêter l'option haute disponibilité sur le firewall en marche, puis arrêter ce firewall,

3. Démarrer le premier firewall, puis arrêter l'option haute disponibilité sur ce firewall.. (éventuellement changer ses IP).

Arrêter la haute disponibilité sur un seul firewall risque de causer des problèmes de conflit d'utilisation d'adresses IP et Mac.

© Copyright NETASQ 2006

Lorsque vous tentez de vous connecter au cluster (ensemble des deux firewalls) via le Firewall Manager ou firewall Monitor, la connexion est forcément établie avec le firewall actif. Pour se connecter au firewall passif, il faut rendre ce dernier actif (en utilisant le bouton « Permuter » de l'onglet « Configuration »).

La synchronisation des firewalls après une modification de la configuration du firewall actif entraîne un reboot du firewall passif.

Les fichiers de traces ne sont pas communs. Vous ne verrez dans un fichier que les traces récupérées lorsque le firewall était actif. Pour centraliser les logs des deux firewalls, il faut les rediriger vers un serveur SYSLOG externe identique, vers le serveur NETASQ SYSLOG ou vers le NETASQ Log Analyzer.

Une sauvegarde du système complet (sur la partition de back up) ne sera réalisée que sur le firewall actif.

Pour tester la haute disponibilité, vous pouvez débrancher une interface réseau du firewall actif, le second firewall doit, au bout d'un temps donné, basculer en actif.

Processus de mise à jour

Pour mettre à jour vos firewalls en haute disponibilité, il y a deux possibilités :

► la mise à jour par le firewall actif,
► la mise à jour par le firewall passif (réalisable que pour une mise à jour mineure à partir de la version 5).

La mise à jour par le firewall actif

Lorsqu'une mise à jour logicielle du firewall actif est réalisée, il n'y a pas de permutation lors du redémarrage du firewall actif.

Une fois que le firewall actif a été mis à jour, vous devez réaliser une permutation manuelle des deux firewalls en cliquant sur le bouton "Permuter" de l'onglet "Configuration".

Déconnectez puis reconnectez-vous (vous serez alors connecté sur l'autre firewall).

Réalisez à nouveau la mise à jour logicielle. Le reboot consécutif entraînera une permutation des firewalls pour se retrouver dans la configuration précédant la mise à jour.

Cette procédure permet de récupérer au moins un firewall dans l'ancienne version logicielle, si la mise à jour ne s'est pas déroulée correctement.

La mise à jour par le firewall passif

L'option « Mise à jour du passif » de l'assistant de mise à jour du firewall (cf Chapitre IX) vous permet de mettre à jour la firewall passif avant le firewall actif. Dans ce cas vous mettez à jour le firewall passif à partir du firewall actif.

Puis une fois le firewall passif redémarré vous pouvez pratiquer une permutation manuelle pour réitérer l'opération (mise à jour du passif).

Puis une fois le deuxième firewall redémarré vous pouvez permuter manuellement les firewalls pour retrouver dans la configuration précédant la mise à jour.

Cette procédure permet de récupérer au moins un firewall dans l'ancienne version logicielle, si la mise à jour ne s'est pas déroulée correctement sans altérer la continuité des services.

© Copyright NETASQ 2006

Chapitre IX

Gestion des traces

© Copyright NETASQ 2006

Section A

Configuration des traces

© Copyright NETASQ 2006

Introduction

Pour cette section, vous devez avoir franchi les étapes

► Interface graphique,
► Installation, intégration et pré-configuration,
► Définition des interfaces, des objets et de la configuration du noyau,
► Mise en place des politiques (translations, filtrage, VPN),
► Configuration des proxies,
► Configuration de l'authentification,
► Haute disponibilité.

Pour cette section, vous devez connaître

► La façon dont vous voulez être informé des alarmes,
► Les statistiques dont vous avez besoin.

Utilité de la section

Cette section vous permet de configurer la gestion des différents fichiers de traces et de configurer les statistiques. Elle vous permet aussi de rediriger les traces vers un serveur SYSLOG externe.

Introduction à cette section

L'IPS-Firewall gère un certain nombre de fichiers de trace destinés à recueillir les événements détectés par les fonctions de journalisation. Les fichiers concernés par les événements de sécurité sont :

► Filtres : événements liés à l'application des fonctions de filtrage,
► VPN : événements liés à l'établissement des SA,
► Alarmes : événements liés à l'application des fonctions de prévention des intrusions,
► Authentification : événements liés à l'authentification des utilisateurs,
► Histo Manager : événements liés à l'authentification des administrateurs et aux opérations d'administration de la sécurité,
► Système : arrêt/démarrage des fonctions de journalisation. Plus généralement :c'est dans ce journal que sont enregistrés les événements liés directement au système : arrêt/démarrage de l'IPS-Firewall, erreur système, etc. L'arrêt et démarrage des fonctions de journalisation correspondent à l'arrêt et au démarrage des « démons » qui génèrent les traces.

Les fichiers Filtres, VPN, Alarmes et Système partagent un espace global de stockage avec d'autres fichiers de traces. L'administrateur possédant les droits « *+M » peut spécifier le pourcentage maximum que chacun des fichiers de trace peut occuper dans cet espace total.

© Copyright NETASQ 2006

Lorsque le seuil maximum est atteint, l'IPS-Firewall entreprend une action paramétrée, pour chaque fichier, parmi les trois suivantes :

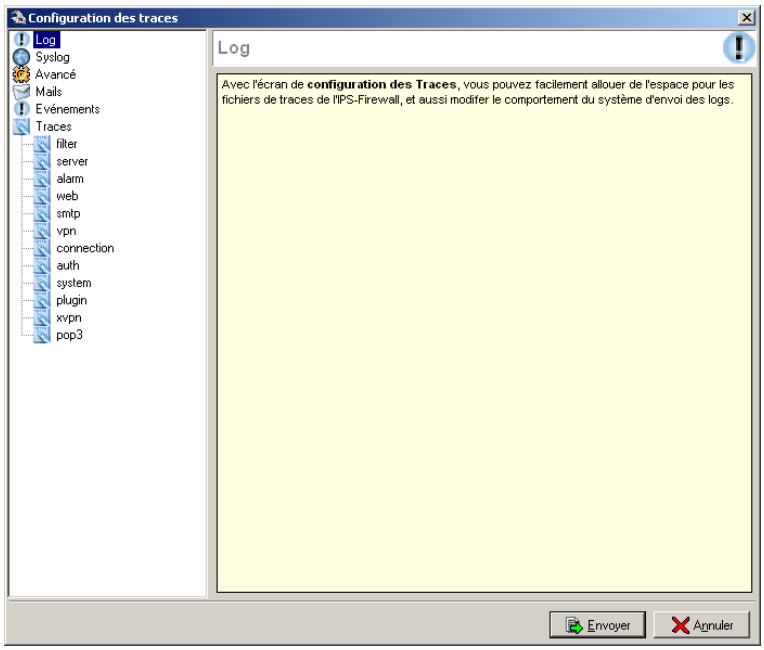
► Rotation des fichiers : les traces les plus récentes effacent les traces les plus anciennes,
► Stopper l'écriture des fichiers : les traces ne sont plus mémorisées sur l'IPS-Firewall,
► Arrêter le Firewall : l'IPS-Firewall ne s'arrête pas réellement mais il bloque l'ensemble des flux excepté les connexions du Firewall Manager depuis le réseau interne.

Les fichiers « Authentification » et « Histo Manager » ont chacun un espace alloué fixe et sont protégés par des actions de rotation en cas de saturation.

Accéder à cette section

Accédez à la boîte de dialogue par le menu « Traces » de l'arborescence.

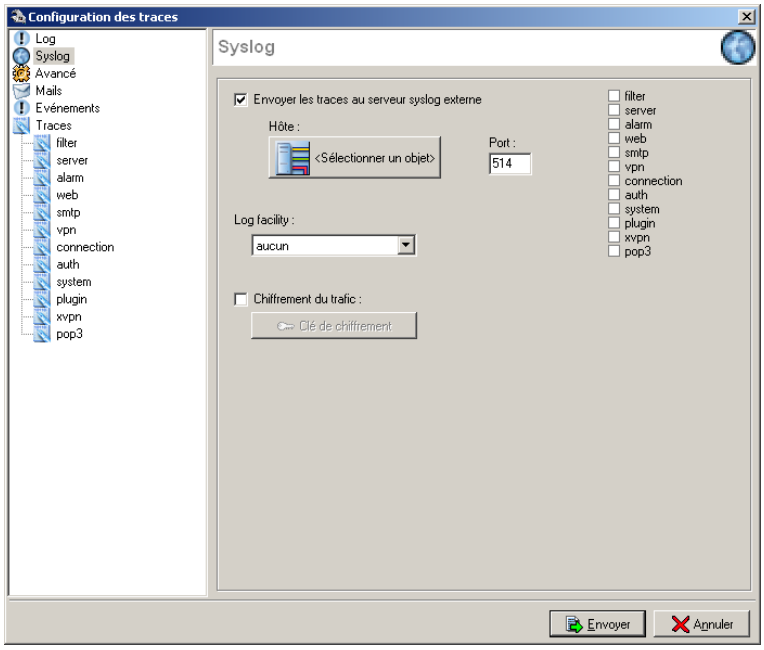
En sélectionnant le menu « Traces » de l'arborescence de l'interface graphique de configuration NETASQ, l'écran de configuration des traces apparaît.



Cet écran est divisé en deux parties :

► A gauche un arbre présentant les diverses fonctionnalités du menu Traces,
► A droite les options configurables.

Menu Syslog



Envoi des traces vers un serveur externe

Le Firewall NETASQ vous permet d'envoyer automatiquement les traces vers un serveur dédié. Les traces sont envoyées au format WELF. Ce serveur peut être un serveur SYSLOG ou le NETASQ SYSLOG. Les traces peuvent aussi être récupérées par le NETASQ LOG ANALYZER.

Pour envoyer les traces, il suffit de cocher la case "Envoyer les messages au serveur syslog externe" puis de donner l'adresse IP du serveur ainsi que le port de communication associé au serveur .

Vous pouvez aussi sélectionner le niveau de facility (c'est un aiguillage vers différents fichiers afin de trier les informations) sur lequel sont envoyées les traces ainsi que les catégories de fichiers à envoyer (Alarme, connexion, web, filtrage…).

Envoi des traces vers le NETASQ SYSLOG ou le NETASQ LOG ANALYZER

Le NETASQ SYSLOG est un utilitaire installé sur une machine d'administration qui offre un service SYSLOG pour la récupération et la gestion de traces. Cet utilitaire est particulièrement intéressant pour les firewalls F50 qui ne peuvent pas stocker les traces sur le firewall. Les traces sont alors stockées en local sur la machine d'administration.

Le NETASQ LOG ANALYZER est un outil plus évolué développé par NETASQ et disponible en option. Il peut récupérer les logs de différents Firewalls et les stocker dans une base SQL, apportant plus de performance dans les traitements de données.

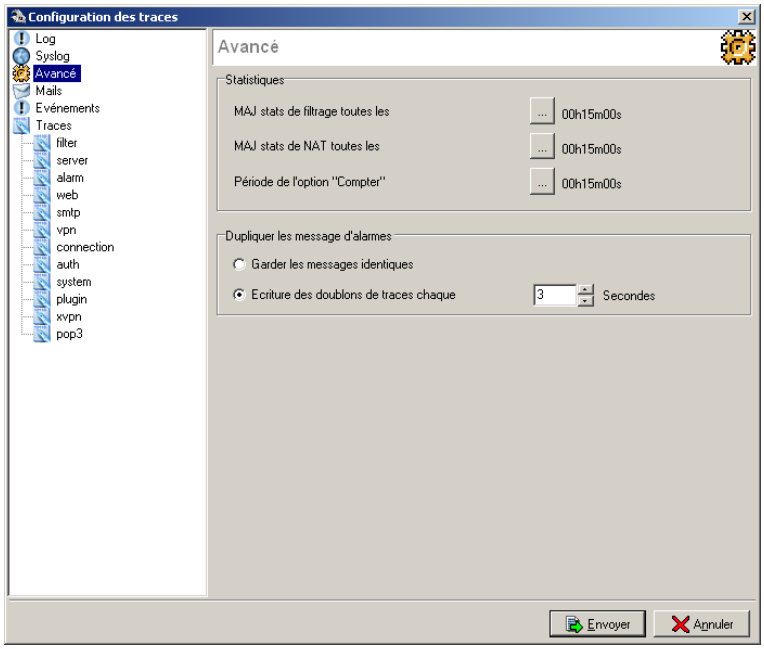
Les traces peuvent être envoyées au NETASQ Syslog en indiquant l'adresse IP de la machine sur laquelle est installé l'outil ainsi que le port utilisé.

Les communications entre le firewall et le NETASQ SYSLOG peuvent être chiffrées en AES à partir du firewall. Pour cela, activez l'option "Chiffrement du trafic" et indiquez la clé de chiffrement utilisée en cliquant sur le bouton "Clé de chiffrement".

Le chiffrement n'est utilisable que pour une redirection des logs vers le NETASQ SYSLOG et pas pour un serveur SYSLOG quelconque. L'option "Chiffrement du trafic" doit donc être désactivée pour un serveur Syslog quelconque. Par contre il est fortement conseillé d'activer le chiffrement pour le Syslog NETASQ. Les communications entre les firewalls et le Log Analyzer sont elles toujours chiffrées.

Les traces peuvent aussi être conservées sur le Firewall (sauf modèle F50).

Menu Avancé



Statistiques

Ce menu vous permet de configurer plusieurs types de statistiques :

► Configuration des statistiques du filtrage,
► Configuration des statistiques de la translation d'adresse,
► Taux de rafraîchissement des règles de filtrage contenant l'option « Compter ».

Pour chaque partie il vous suffit de sélectionner la fréquence du calcul des statistiques. Un rapport sera généré pour chaque période que vous configurez.

Une fois vos choix effectués, appuyez sur le bouton "Envoyer" pour envoyer les informations au Firewall NETASQ.

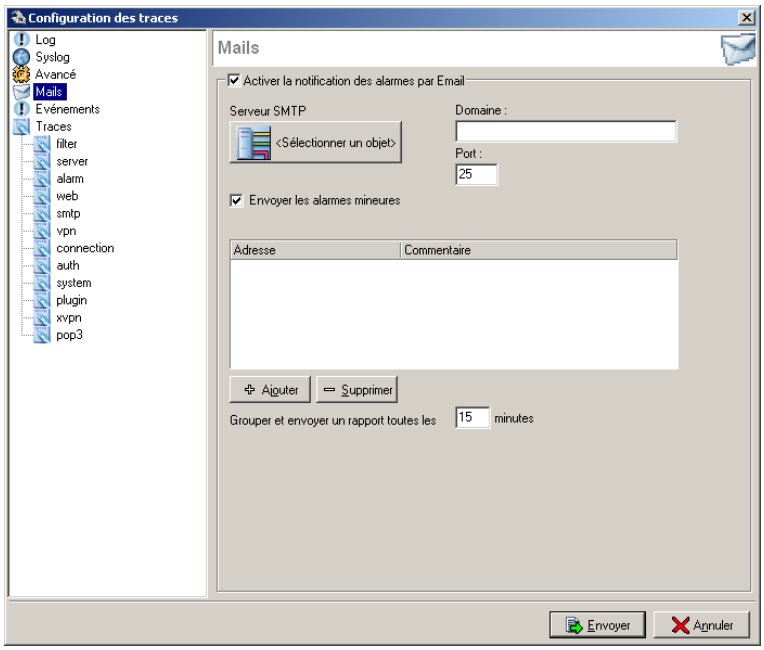
Nous vous conseillons de n'utiliser les granularités inférieures à une journée que sur une courte durée afin d'éviter de saturer le disque du Firewall NETASQ.

Dupliquer les messages d'alarmes

Deux options concernant les « Dupliquer les messages d'alarmes » sont disponibles dans le menu avancé :

► Garder les messages identiques : dans ce cas toutes les alarmes sont inscrites dans les logs (même si elles sont identiques),
► Ecriture des doublons de traces chaque : ici vous sélectionnez une fenêtre de temps dans laquelle même si une alarme est remontée plusieurs fois, elle n'est inscrite qu'une seule fois dans les logs.

Ce menu vous permet de configurer la réception des alarmes sur une ou plusieurs adresses de courrier électronique.



L'écran de configuration comporte les champs suivants :

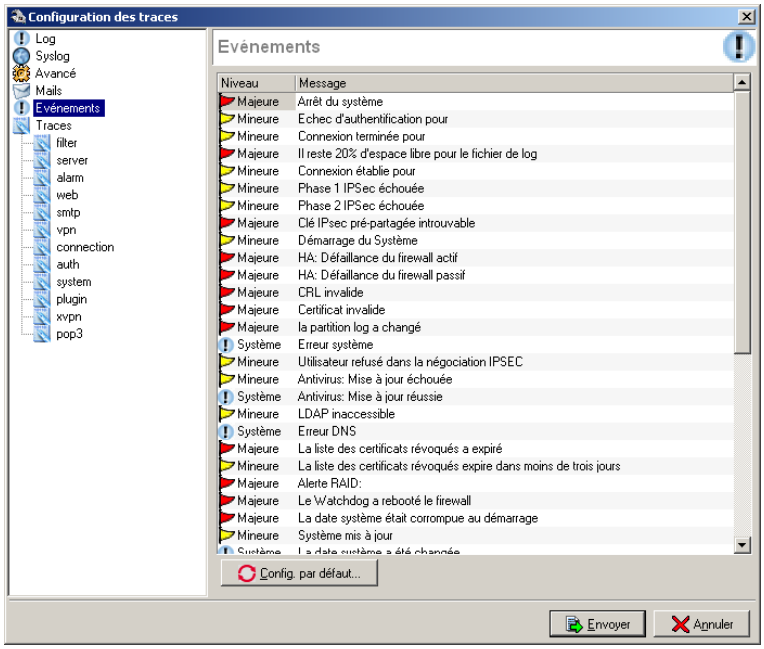
Activer la notification des alarmes par e-mail	Active l'envoi des messages d'alarmes sur les e-mails spécifiés.
Serveur SMTP (IP)	Adresse IP du serveur SMTP où seront envoyés les e-mails.
Port	Port du serveur SMTP où seront envoyés les e-mails.
Domaine	Domaine interne des adresses électroniques.
Envoyer les alarmes mineures	Active l'envoi des alarmes mineures. Par défaut seules les alarmes majeures sont envoyées.
Liste de diffusion	Liste des adresses qui recevront les alarmes. Vous pouvez modifier la liste avec les boutons Ajouter/Retirer se situant sous cette liste.
Grouper et envoyer un rapport toutes les	Cette option vous permet de préciser le temps d'attente entre l'envoi de deux messages d'alarme pour la même attaque. Ceci évite de saturer de messages la boîte aux lettres en cas d'afflux d'attaques du même type.

Il n'est pas nécessaire de configurer de règle de filtrage pour l'envoi de ces e-mails.

Certains serveurs de courrier externes utilisent des IP multiples. Dans ce cas, il convient de contacter le fournisseur d'accès. Vous pouvez vous connecter à un serveur sur votre réseau interne en IP fixe.

© Copyright NETASQ 2006

Ce menu vous permet de modifier les actions par défaut à entreprendre lors de la remontée de certains types d'événements. Ceux-ci sont indépendants des conditions de trafic. La liste présentée dans cette fenêtre regroupe tous les événements que peut générer un IPS-Firewall.



La grille se divise en deux :

- ► à gauche figurent les actions à entreprendre lors de la remontée d'un événement,
- ► à droite figure le type d'événement.

Les différentes actions possibles sont :

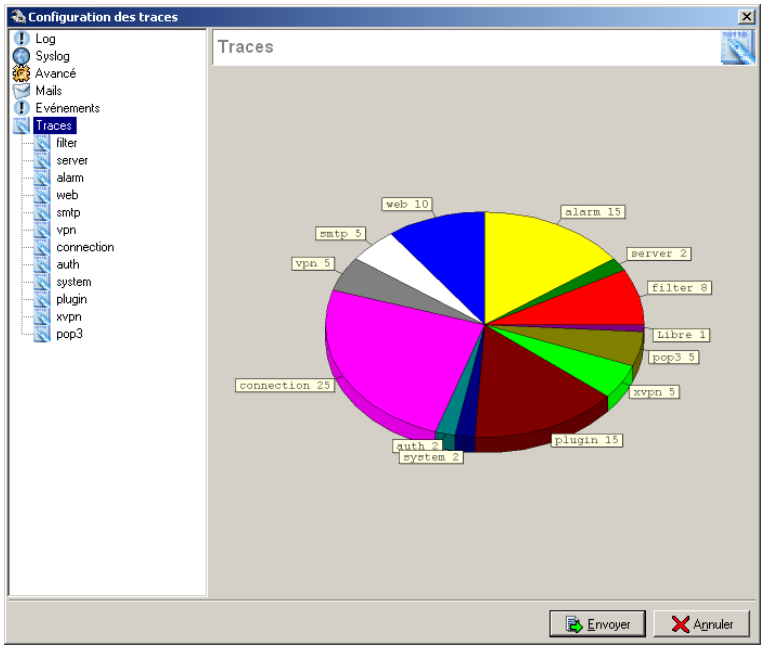
Ignorer	Aucune notification.
Mineure	Génère une alarme mineure.
Majeure	Génère une alarme majeure.
Système	Génère une entrée dans le journal d'audit système.

Le bouton « Configuration par défaut » vous permet de redéfinir les paramètres d'événements dans leur configuration d'origine.

Une fois vos modifications effectuées, vous devez les envoyer au Firewall NETASQ avec le bouton « Envoyer ».

© Copyright NETASQ 2006

Ce menu vous donne la possibilité de configurer plusieurs paramètres liés aux traces: leur taille, l'action à entreprendre lorsque le seuil est atteint, etc. Lorsque vous sélectionnez ce menu, la fenêtre principale du menu vous présente un aperçu graphique de la répartition actuelle de l'espace réservé pour chacun des fichiers de traces.



Gestion des fichiers de traces

Pour chaque menu de traces (filter, server, alarm, WEB, SMTP, VPN, connection, auth, system, plugin, xvpn, pop3 et monitor), vous pouvez limiter la taille du fichier de traces du filtrage en sélectionnant la taille du fichier en pourcentage de l'espace réservé pour les fichiers de logs.

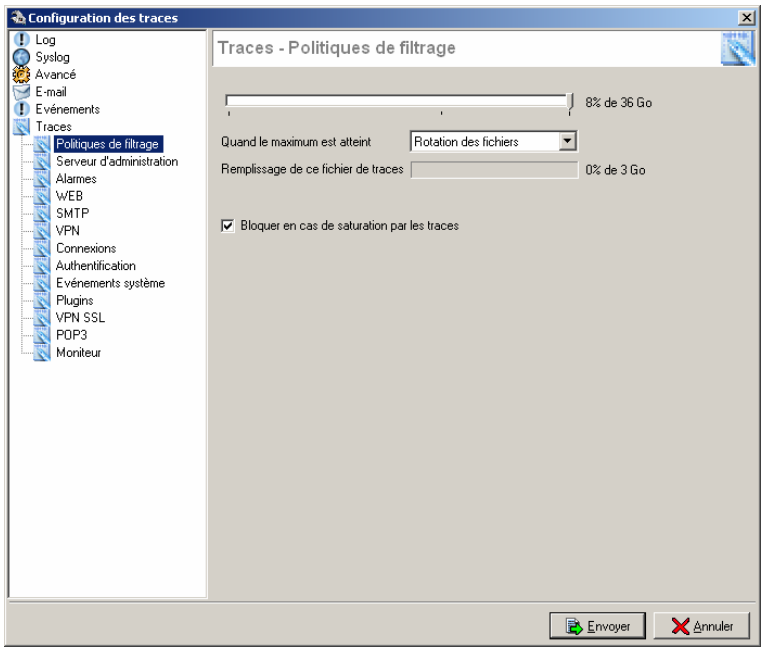
Vous avez aussi la possibilité de choisir l'action à entreprendre une fois que ce seuil est atteint. Les différentes possibilités sont :

► Rotation des fichiers : les traces les plus récentes effacent les traces les plus anciennes,
► Stopper l'écriture des fichiers : les traces ne sont plus mémorisées sur le Firewall,
► Arrêter le Firewall : le Firewall ne s'arrête pas réellement mais il bloque l'ensemble des flux exceptés les connexions du Firewall Manager depuis le réseau interne.

Enfin un graphique représente le taux d'occupation actuel en pourcentage.

© Copyright NETASQ 2006

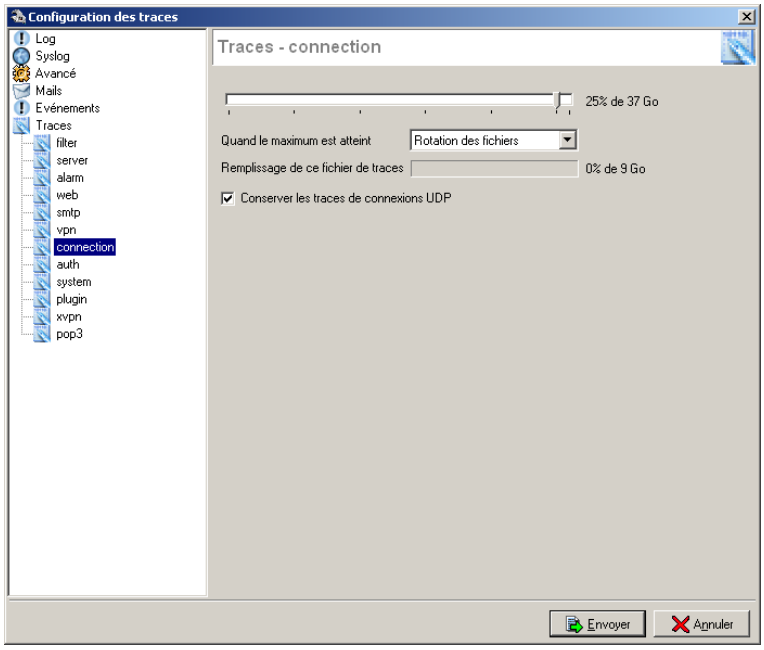
Bloquer en cas de saturation par les traces



L'option « Bloquer en cas de saturation par les traces », présente dans les menus « Politiques de filtrages » et « Alarmes » définit qu'un trafic autorisé par le filtrage à traverser l'appliance sera tout de même bloqué si l'enregistrement dans les traces est impossible (espace réservé plein ou surcharge de l'appliance par exemple). Cette condition ne s'applique que sur les trafics passants avec l'option « tracer » appliquée à la règle.

En décochant cette option, vous permettez que les trafics passants (ET dont l'option « Tracer » est spécifiée) soient autorisés même si l'enregistrement des traces (logging) est impossible.

Conserver les traces de connexions UDP



L'option « Conserver les traces de connexions UDP », présente dans le menu « connection », permet de tracer aussi les datagrammes UDP. Attention, de part la nature de ce type de flux (un envoi datagramme = 1 connexion), les traces peuvent être plus rapidement engorgées.

Section B

Réception des alarmes et des traces

© Copyright NETASQ 2006

Le Firewall NETASQ différencie deux types d'alarmes :

► Les alarmes majeures,
► Les alarmes mineures.

Les alarmes mineures sont déclenchées par les paquets arrivant au Firewall NETASQ et correspondant à une règle de filtrage ou à un événement pour laquelle ou lequel vous avez spécifié l'action "Alarme mineure".

Les alarmes majeures sont déclenchées automatiquement par le Firewall NETASQ lorsqu'un paquet ou une action lui semble réellement suspect. Par exemple : une attaque par SYN Flooding.

Plusieurs moyens permettent d'être informé des alarmes émises par le Firewall :

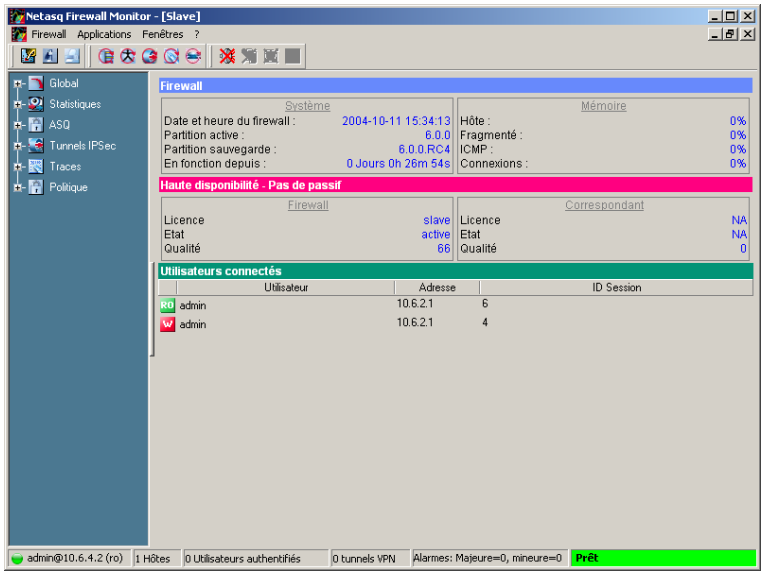
► Un voyant s'allume ou clignote suivant le type d'alarme sur la face avant du Firewall NETASQ (disponible seulement sur certains boîtiers),

► l'alarme est envoyée aux moniteurs temps réel connectés. Pour recevoir les alarmes sur un poste distant, il faut lancer le moniteur temps réel et ouvrir une connexion vers le Firewall à surveiller,

► par e-mail. Pour cela, il faut remplir le champ « Serveur SMTP » avec l'adresse IP du serveur SMTP. Vous pouvez ensuite préciser l'adresse e-mail de réception des messages d'alarmes.

© Copyright NETASQ 2006

Dans le répertoire où se trouve le logiciel de configuration depuis Windows (« C:\Program Files\Netasq\Administration Suite x.x » par défaut) vous trouverez l'application « monitor.exe » ou tout simplement à partir du raccourci « Applications > Firewall Moniteur » dans la barre de menus.



Le moniteur d'alarmes temps réel vous permet de visualiser simplement les connexions transitant par le Firewall et les alarmes qu'il a déclenchées.

Lorsqu'il est connecté, le moniteur reçoit les informations du Firewall. Vous pouvez ensuite le réduire avec le bouton de réduction de la fenêtre Windows. Le moniteur tourne alors en arrière plan. Pour le faire réapparaître à l'écran, double cliquez sur l'icône figurant au niveau de la barre des tâches (à côté de l'horloge).

Par défaut, ce moniteur ne peut être exécuté que sur une machine connectée au réseau interne et doit être lancé en permanence pour ne pas perdre d'alarmes. Vous pouvez l'utiliser de façon distante (au travers d'Internet) mais il faut alors explicitement autoriser le service (Firewall_srv), dans les règles de filtrage.

Pour une description complète du Moniteur, veuillez vous reporter la suite du document dans le Chapitre XII « Moniteur Temps réel ».

© Copyright NETASQ 2006

A la réception d'une alarme, la fenêtre du Firewall Monitor peut passer en avant-plan et un son est éventuellement émis.

Dans le cas où une alarme ne parvient pas au moniteur, celle-ci est tout de même tracée et le voyant "minor" située en face avant du Firewall NETASQ est allumé brièvement. De plus, si vous avez précisé une adresse mail où envoyer les alarmes, les messages d'alertes seront envoyés par mail.

La génération d'alarmes est très pratique pour pister d'éventuels abus. Il suffit, pour cela, d'ajouter, dans les règles de filtrage, l'option "alarme mineure" sur la règle dont vous voulez pister l'utilisation. Cependant une utilisation excessive de cette fonctionnalité la rendra très rapidement inutilisable de part la taille des fichiers de traces générées, le nombre d'alarmes affichées sur votre moniteur et le passage en avant-plan de la fenêtre du moniteur.

© Copyright NETASQ 2006

Chapitre X

Sauvegarde et mise à jour

© Copyright NETASQ 2006

Pour cette section, vous devez avoir franchi les étapes

► Interface graphique,
► Installation, intégration et pré-configuration.

Pour cette section, vous devez connaître

► L'adresse IP du Firewall NETASQ sur le réseau interne.

Utilité de la section

Cette section vous permet de sauvegarder / restaurer toutes les informations spécifiques à votre Firewall.

L'administrateur possédant le droit « maintenance » peut sauvegarder dans un fichier sur la station d'administration :

► la configuration complète,
► la configuration réseau de l'IPS-Firewall (adresses de l'IPS-Firewall, passerelles, etc.),
► les objets (machines, réseaux, services et chacun des groupes),
► les règles de filtrage,
► la base LDAP (base locale des utilisateurs).

Il est possible de chiffrer et signer le fichier avec un mot de passe.

La restauration de la configuration à partir d'un fichier de sauvegarde nécessite les droits de maintenance.

Enfin, cette section explique la méthode de mise à jour des boîtiers.

Accéder à cette section

Accédez aux boîtes de dialogue par les sous-menus « Maintenance > Sauvegarde », « Maintenance > Restauration », « Maintenance > Mise à jour » et « Maintenance > Mise à jour WEB ».

Vous devez être connecté avec les privilèges de modification pour pouvoir effectuer ces modifications.

© Copyright NETASQ 2006

Lorsque vous apportez des modifications à votre Firewall, pour des raisons de sécurité, aucune information n'est enregistrée sur l'ordinateur où est installé le firewall Manager.

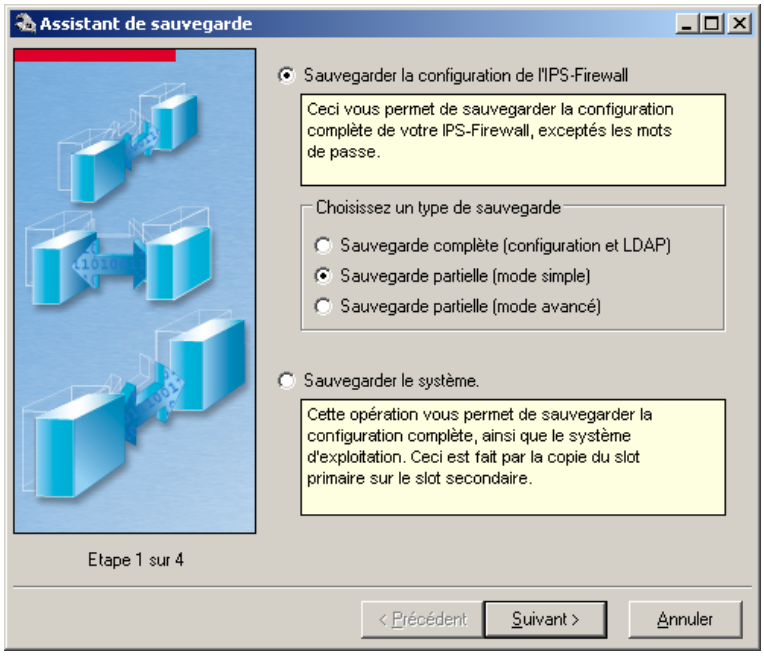
Ceci présente en outre un autre avantage : vous pouvez consulter et configurer le Firewall à partir de n'importe quel poste du réseau interne équipé de l'interface graphique.

Toutefois, il est important de constater que ceci présente un inconvénient : en cas d'erreur lors de la configuration, de problème hardware ou, si vous voulez configurer plusieurs Firewalls de manière presque identique vous êtes plus ou moins bloqué.

C'est pourquoi le firewall Manager est équipé d'une fonctionnalité permettant de sauvegarder/restaurer l'ensemble ou une partie des fichiers de configuration de votre Firewall. La sauvegarde réalisée peut être chiffrée et signée pour des raisons de confidentialité et d'intégrité de la configuration.

Sauvegarde de la configuration

Pour sauvegarder la configuration de l'appliance NETASQ, sélectionnez le sous-menu « Maintenance > Sauvegarde » de la barre de menu située en haut de l'interface Firewall Manager. Un assistant vous guide pas à pas dans les fonctionnalités de sauvegarde des produits NETASQ.


Assistant de sauvegarde
Sauvegarder la configuration de l'IPS-Firewall
Ceci vous permet de sauvegarder la configuration complète de votre IPS-Firewall, exceptés les mots de passe.
Choisissez un type de sauvegarde
Sauvegarde complète (configuration et LDAP)
Sauvegarde partielle (mode simple)
Sauvegarde partielle (mode avancé)
Sauvegarder le système.
Cette opération vous permet de sauvegarder la configuration complète, ainsi que le système d'exploitation. Ceci est fait par la copie du slot primaire sur le slot secondaire.
Etape 1 sur 4
< Précédent
Suivant >
Annuler

La première étape permet de définir ce qui doit être sauvegardé : la configuration ou le système. Comme indiqué dans l'interface, la sauvegarde de la configuration consiste à enregistrer sur la station d'administration un fichier chiffré contenant la configuration de l'appliance (totale ou partielle selon les options choisies). La sauvegarde du système consiste à enregistrer sur l'appliance directement, dans une partition de sauvegarde, l'ensemble du système et de la configuration.

Cette section s'intéresse à la sauvegarde la configuration.

© Copyright NETASQ 2006

Type de sauvegarde de configuration

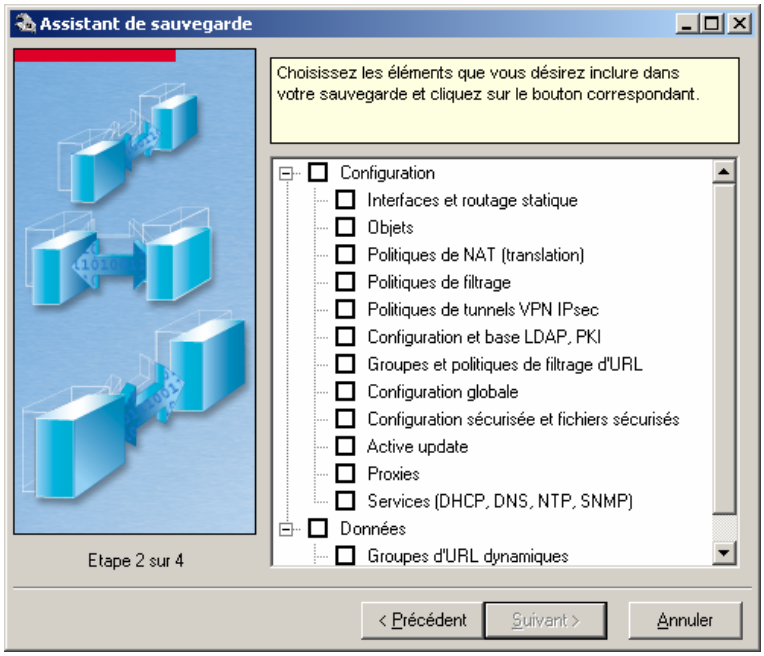
Il existe trois types de sauvegarde de la configuration :

► **Sauvegarde complète (configuration et LDAP)** : ce choix permet la sauvegarde de la configuration de l'appliance et de l'ensemble des informations stockées dans la base LDAP (fiches utilisateurs), sans option, cette configuration enregistre tout.

► **Sauvegarde partielle (mode simple)** : ce choix permet la sauvegarde de la configuration de l'appliance selon des choix effectués par l'administration. Ce type de configuration partielle permet par exemple l'enregistrement de la base d'objets pour que celle-ci soit ensuite restaurer sur un autre produit et ainsi faciliter le travail de l'administrateur.

► **Sauvegarde partielle (mode avancé)** : ce choix, plus granulaire que l'option « simple » permet la sélection la plus spécifique en terme de sauvegarde.

Options de la sauvegarde simple



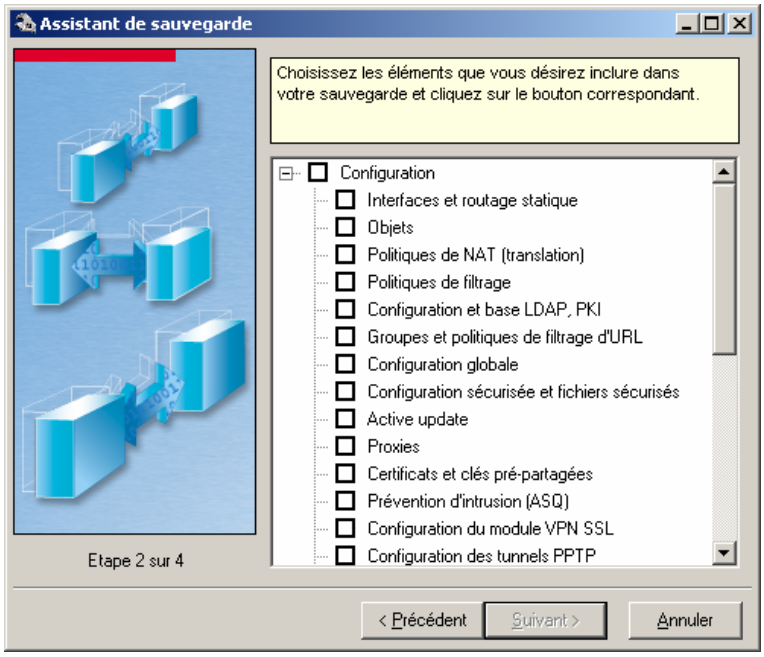
Lorsque la sauvegarde simple est sélectionnée, les options de sauvegarde sont les suivantes :

► **Configuration** : sélectionne tous les élements situés sous ce choix.
► **Interfaces et routage statique** : configuration réseau de l'appliance, la configuration des interfaces, la passerelle par défaut et les routes statiques.
► **Objets** : la base des objets, sauf les utilisateurs.
► **Politiques de NAT** : tous les slots de la configuration de la translation d'adresses.
► **Politiques de filtrage** : tous les slots de la configuration du filtrage.
► **Politiques de tunnels VPN IPsec** : tous les slots de la configuration des tunnels VPN IPsec, les clés pré partagées et les certificats stockés dans le menu « Certificats ».
► **Configuration et base LDAP, PKI** : configuration de la base LDAP de l'appliance, ainsi que les élements stockés dans la base (utilisateurs) et configuration de la PKI.
► **Groupes et politiques de filtrage d'URL** : tous les slots de la configuration du filtrage d'URL ainsi que les groupes d'URL statiques (créés par l'administrateur).
► **Configuration globale** : tous les slots de la configuration globale ainsi que les objets globaux.
► **Configuration sécurisée et fichiers sécurisés** : configuration sécurisée et fichiers chiffrés et sécurisés par la configuration sécurisée.
► **Active Update** : configuration du module de mise à jour automatique de l'appliance.
► **Proxies** : configuration des proxies HTTP, SMTP et POP3.
► **Services** : configuration des services de l'appliance, DHCP, DNS, NTP et SNMP.
► **Données** : sélectionne tous les éléments situés sous ce choix.

© Copyright NETASQ 2006

► **Groupes d'URL dynamiques** : tous les groupes d'URL dynamiques, obtenus par Active Update.
► **Signatures contextuelles** : signatures ASQ obtenues par Active Update.

Options de la sauvegarde avancée



Lorsque la sauvegarde avancée est sélectionnée, les options de sauvegarde sont les suivantes :

► **Configuration** : sélectionne tous les élements situés sous ce choix.
► **Interfaces et routage statique** : configuration réseau de l'appliance, la configuration des interfaces, la passerelle par défaut et les routes statiques.
► **Objets** : la base des objets, sauf les utilisateurs.
► **Politiques de NAT** : tous les slots de la configuration de la translation d'adresses.
► **Politiques de filtrage** : tous les slots de la configuration du filtrage.
► **Configuration et base LDAP, PKI** : configuration de la base LDAP de l'appliance, ainsi que les élements stockés dans la base (utilisateurs) et configuration de la PKI.
► **Groupes et politiques de filtrage d'URL** : tous les slots de la configuration du filtrage d'URL ainsi que les groupes d'URL statiques (créés par l'administrateur).
► **Configuration globale** : tous les slots de la configuration globale ainsi que les objets globaux.
► **Configuration sécurisée et fichiers sécurisés** : configuration sécurisée et fichiers chiffrés et sécurisés par la configuration sécurisée.
► **Active Update** : configuration du module de mise à jour automatique de l'appliance.
► **Proxies** : configuration des proxies HTTP, SMTP et POP3.
► **Certificats et clés pré partagées** : certificats stockés dans le menu « Certificats » et clés pré partagées configurées.
► **Prévention d'intrusion (ASQ)** : configuration du moteur de prévention de l'appliance, l'ASQ
► **Configuration du module VPN SSL** : configuration du module VPN SSL.
► **Configuration des tunnels PPTP** : configuration du serveur PPTP.
► **Tunnels VPN IPsec** : configuration des tunnels VPN IPsec uniquement.
► **Programmation horaire** : programmation horaire définie pour les slots.
► **Règles événementielles** : règles de filtrage événementielles configurées manuellement par l'administrateur.
► **QoS** : configuration des politiques de Qualité de Service.
► **Authentification** : configuration de l'authentification.
► **Indicateurs (système et sécurité)** : indicateurs que l'on retrouve dans l'Administration globale.
► **Serveur DHCP** : service DHCP de l'appliance.
► **Client NTP** : service NTP de l'appliance.
► **Proxy DNS** : service DNS de l'appliance.
► **Agent SNMP** : service SNMP de l'appliance.

© Copyright NETASQ 2006

► **Traces** : configuration des traces uniquement.
► **Routage statique** : passerelle par défaut et routes statiques configurées.
► **Evénéments système** : configuration des événéments système.
► **Routage dynamique** : configuration de la plateforme de routage dynamique.
► **Antispam** : module Antispam.
► **Communication (syslog, envoi de notification)** : module de communication de l'appliance, notamment envoi des traces auprès des serveurs syslog et envoi des notifications d'alarmes aux administrateurs.
► **Données** : sélectionne tous les éléments situés sous ce choix.
► **Groupes d'URL dynamiques** : tous les groupes d'URL dynamiques, obtenus par Active Update.
► **Signatures contextuelles** : signatures ASQ obtenues par Active Update.

Options diverses de la sauvegarde

Lorsque les éléments à sauvegarder sont définis (sauvegarde complète ou partielle), il est encore possible de définir quelques options de sauvegarde :

► Description de la sauvegarde. Cette description sera affichée lors de la restauration de la configuration. Ainsi, vous pouvez réaliser plusieurs sauvegardes et distinguer chacune d'entre elles.

► Vous avez aussi la possibilité de chiffrer la sauvegarde afin qu'elle ne puisse pas être restaurée sur un autre firewall ou pour qu'elle ne puisse pas être visualisée. Pour cela, indiquez un mot de passe qui servira pour le chiffrement.

Vous donnez le nom de votre sauvegarde et choisissez son emplacement.

Si la sauvegarde n'est pas stockée sur des supports fiables et sécurisés, il est vivement conseillé d'activer le chiffrement.

Restauration de la configuration

Pour restaurer une configuration sur un appliance NETASQ, sélectionnez le sous-menu « Maintenance > Restauration » de la barre de menu située en haut de l'interface Firewall Manager. Un assistant vous guide pas à pas dans les fonctionnalités de restauration des produits NETASQ.

Dans la première étape de l'assistant, seule la restauration de la configuration est disponible, cvliquez sur suivant pour continuer.

Dans la deuxième étape, indiquez lui le fichier de sauvegarde que vous voulez restaurer. Une description de la sauvegarde s'affiche et vous permet de distinguer les différentes sauvegardes. Puis les options de restauration apparaissent. De la même façon que pour la sauvegarde de configuration, il existe trois types de restauration, ces trois types font référence aux trois types de sauvegarde. Reportez-vous à la section « Sauvegarde de configuration » pour plus d'informations.

Remarques

Il vous est conseillé d'effectuer une sauvegarde des fichiers de configuration à chaque grosse modification.

Si vous ne désirez sauvegarder qu'un slot, vous pouvez utiliser la fonctionnalité copier/coller.

Les mots de passe ne sont pas sauvegardés. Ils restent les mêmes après une sauvegarde ou une restitution.

Cette fonctionnalité n'est pas disponible sur les boîtiers F50. En effet, il n'y a pas de disque dur sur les machines de cette gamme. La copie du système sur une partition n'est donc pas possible.

Cette fonctionnalité vous permet de sauvegarder l'ensemble de la configuration et le système d'exploitation du firewall (image disque). Cela permet de basculer sur cette sauvegarde lors du non-fonctionnement du système principal (problème sur le disque dur, mise à jour infructueuse...).

Une fois que votre configuration est en production sans problème, vous pouvez faire une sauvegarde du système.

La sauvegarde du système peut entraîner une baisse des performances du firewall pendant le temps de la sauvegarde (environ 1 minute).

En cas de problème, vous rebootez et démarrez sur le système de sauvegarde.

Pour cela, il suffit d'être connecté en mode console (clavier + écran) au moment du boot. Lorsque vous voyez apparaître le menu de démarrage, tapez 2 pour démarrer sur la sauvegarde.

Une fois le firewall démarré, vous pouvez vous y connecter avec l'interface graphique pour rétablir le système de sauvegarde sur le système principal.

© Copyright NETASQ 2006

Deux types de mise à jour peuvent être faites :

► Mise à jour du logiciel firewall,
► Mise à jour de l'interface graphique de configuration (Firewall Manager et Firewall Monitor).

La mise à jour de fonctionnalités logicielles du Firewall NETASQ est une opération de maintenance. Vous comprendrez que la mise à jour des fichiers système sur le Firewall NETASQ soit une opération délicate et entraîne une coupure du service pour les utilisateurs.

Vous devez toujours réaliser la mise à jour dans l'ordre suivant :

1. Mise à jour du logiciel firewall à partir de l'ancienne interface graphique,

2. Désinstallation de l'ancienne interface graphique de configuration si vous ne désirez pas la conserver,

3. Installation de la nouvelle interface graphique de configuration.

Dans le cas des mises à jour majeures, il est important de suivre l'ordre des mises à jour logicielles, le passage d'une version ancienne à une version beaucoup plus récente sans passer par les mises à jour intermédiaires sera bloquée par le firewall.

Mise à jour de l'interface graphique

Cette mise à jour consiste en une simple réinstallation du logiciel.

Il vous suffit d'avoir préalablement récupéré l'installation sur le poste où vous désirez l'effectuer et de l'exécuter.

Mise à jour du firewall

La mise à jour du firewall par l'interface graphique est très simple. On y accède par le menu « Fichier > Mise à jour ».

Un assistant vous guide dans la mise à jour de votre IPS-Firewall.

Dans la première étape, celui-ci vous demande la localisation du fichier de mise à jour. Vous devez télécharger ce fichier, portant l'extension .maj à partir du site WEB de NETASQ (www.netasq.com).

Vérifiez les informations de la mise à jour affichées lors de l'insertion du fichier MAJ dans l'assistant.

Vous avez ensuite le message d'avertissement qui vous rappelle que cette mise à jour nécessite de redémarrer le Firewall et donc de couper momentanément les connexions qui le traversent.

Vous voyez aussi, à ce niveau, quelle est la version minimale à avoir pour pouvoir réaliser cette mise à jour.

© Copyright NETASQ 2006

Pendant la mise à jour, une fenêtre de progression s'affiche vous indiquant que la mise à jour est en train de se dérouler.

A la fin de l'envoi du fichier, le message vous indique que le fichier a été transféré et le firewall redémarre.

A la prochaine connexion, vous aurez un message vous indiquant le résultat du changement de version.

Haute disponibilité

Si vous possédez deux firewalls en haute disponibilité, il vous est possible mettre à jour le firewall passif avant le firewall actif (cf chapitre VII « Haute disponibilité »). Cette opération en cochant l'option « Mise à jour du passif » de l'assistant.

Mise à jour certifiée

Pour vérifier si une version ou une mise à jour a bien été certifiée, il faut se connecter sur le site WEB de NETASQ (www.netasq.com), puis se logger sur son compte à partir de l'espace client. Ensuite, dans la partie « Centre de téléchargement », cliquez sur le lien « Les dernières mises à jour » pour vérifier si la dernière version a été certifiée ou sur le lien « Les mises à jour précédentes » pour vérifier les versions certifiées parmi la liste des anciennes mises à jour. Une mention sera alors indiquée pour chaque version certifiée.

Downgrade vers la version 6.1

Une mise à jour inversée (downgrade) peut être réalisée entre une version 6.2 et une version 6.1. L'opération consiste tout simplement à proposer comme mise à jour un fichier maj 6.1 sur un appliance en 6.2. Toutefois cette Downgrade DOIT ETRE SUIVIE D'UNE REMISE EN CONFIGURATION PAR DEFAUT. Cela implique que l'appliance 6.2 qui est mis en 6.1 perd sa configuration. Pour conserver une configuration il est indispensable d'avoir effectué une sauvegarde de configuration dans la version précédant la mise à jour du boitier.

Ainsi pour effectuer une downgrade, reportez-vous à la procédure suivante :

1. Votre appliance est en version 6.1,

2. Effectuer une sauvegarde de la configuration en version 6.1,

3. Mettre à jour votre boitier en version 6.2,

Les étapes 1 à 3 sont les étapes qu'il faut obligatoirement avoir effectué pour pouvoir réaliser une downgrade de votre produit d'une version 6.2 vers une version 6.1.

4. Downgrade : Mettre votre boitier 6.2 en version 6.1,

5. Mettre en configuration par défaut le boitier mis à jour (defaultconfig),

6. Restaurer la configuration sauvegardée.

ATTENTION cette procédure de mise à jour inversée n'est valable que pour un boitier en version 6.2 vers une version 6.1. Si votre configuration ne correspond pas à ce type de version, contactez votre partenaire certifiée pour obtenir les informations adéquates.

Remarques

La procédure de mise à jour n'altère pas vos fichiers de configuration : ceux-ci sont stockés sur le Firewall NETASQ. Les fichiers de configuration sont mis à jour en même temps que le firewall.

La mise à jour de fichiers système sur le Firewall NETASQ n'implique pas systématiquement une mise à jour du logiciel de configuration à distance. Si c'est le cas, cela sera stipulé au moment du téléchargement de la nouvelle version.

Inversement, la mise à jour du logiciel de configuration à distance n'implique pas systématiquement une mise à jour des fichiers système du Firewall NETASQ. Si c'est le cas, cela sera stipulé au moment du téléchargement de la nouvelle version.

Notez qu'il est pas possible d'installer une mise à jour modifiée (erronée, altérée, compromise,…) car le fichier de mise à jour est chiffré et nécessite donc de la part du logiciel de configuration à distance et de l'IPS-Firewall des mécanismes et des clés de déchiffrement pour réaliser l'opération de mise à jour.

L'IPS-Firewall NETASQ est un produit de sécurité qui évolue pour protéger le réseau, de menaces toujours plus évoluées. Des mises à jour régulières sont nécessaires pour prendre en compte ces différentes évolutions. De plus les logiciels de la suite d'administration doivent être mis à jour pour gérer ces nouvelles fonctionnalités.

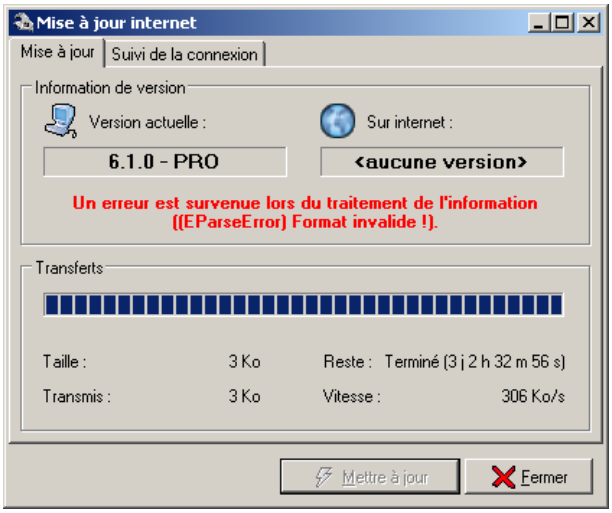
La **recherche des mises à jour** du Firmware ou de la Suite d'Administration peut être effectuée **automatiquement** par des mécanismes de programmation **expliqués dans la section « Préférences \ Web Update »** ou manuellement.

Cette section décrit les menus permettant la recherche manuelle de mises à jour. Pour accéder à ces menus sélectionnez dans les menus du Firewall Manager :

► Maintenance \ Mise à jour WEB \ Chercher des mises à jour de l'Administration Suite : pour déclencher manuellement une recherche des mises à jour concernant la suite d'administration des produits IPS-Firewalls NETASQ.

► Maintenance \ Mise à jour WEB \ Chercher des mises à jour de Firmware : pour déclencher manuellement une recherche des mises à jour concernant les firmwares des produits IPS-Firewalls NETASQ.

Mises à jour de l'Administration Suite et du Firmware


Mise à jour internet
Mise à jour
Suivi de la connexion
Information de version
Version actuelle :
Sur internet :
6.1.0 - PRO
<aucune version>
Un erreur est survenue lors du traitement de l'information
((EParseError) Format invalide !).
Transferts
Taille : 3 Ko
Reste : Terminé (3 j 2 h 32 m 56 s)
Transmis : 3 Ko
Vitesse : 306 Ko/s
Mettre à jour
Fermer

La mise à jour de l'Administration Suite et du Firmware permet le support des nouvelles fonctionnalités disponibles sur l'IPS-Firewall, intégrées par NETASQ pour assurer la protection la plus adaptée aux menaces circulant sur l'Internet.

Informations de mises à jour

De nombreuses informations sur le téléchargement des mises à jour sont affichées par le menu de mises à jour WEB. Ces différentes informations sont décrites dans le tableau suivant :

Onglet Mise à jour

Version actuelle	Donnée informative indiquant la version actuellement installée sur le poste de travail.
Sur internet	Donnée informative indiquant la version actuellement disponible

© Copyright NETASQ 2006

	sur le site WEB NETASQ.
Taille	Taille du fichier à télécharger. Généralement la taille d'une mise à jour de la suite d'administration oscille autour de 50 Mo pour la suite d'administration standard et 70 Mo pour la suite d'administration PRO. Une mise à jour du Firmware des IPS-Firewalls NETASQ oscille quant à elle autour de 10 Mo.
Transmis	Données en octets déjà téléchargées.
Reste	Temps restant estimé pour la réception complète du fichier.
Vitesse	Débit informatif de téléchargement de la mise à jour.

Onglet Suivi de la connexion

Le suivi de la connexion de la mise à jour affiche les différents événements survenus lors de la récupération des informations sur le site WEB NETASQ et cela dans toutes les étapes du téléchargement de la mise à jour (login, mot de passe, connexion, téléchargement).

Procédure de mise à jour de la suite d'administration

Pour effectuer une mise à jour de l'Administration Suite, reportez-vous à la procédure suivante :

1. Renseignez les informations nécessaires à la connexion du Firewall Manager au site WEB NETASQ (voir Section « Préférences ») ;

2. Sélectionnez le menu « Maintenance \ Mise à jour WEB \ Chercher des mises à jour de l'Administration Suite » ;

3. Lorsque le menu apparaît il vous indique s'il existe une version plus récente de la Suite d'Administration actuellement sur le site WEB NETASQ ;

4. Cliquez sur le bouton « Mettre à jour », un dossier de téléchargement est demandé si celui-ci n'a pas été spécifié dans les préférences du Web Update (voir Section « Préférences ») puis la nouvelle suite d'Administration est installée.

Si la mise à jour de la suite d'administration est une mise à jour mineure, la nouvelle suite d'administration sera installée sur la suite d'administration précédente (la suite d'administration précédente est écrasée).

Veillez à la compatibilité de connexion entre la nouvelle suite d'administration et l'IPS-Firewall. En effet NETASQ ne garantit pas la compatibilité entre version majeure.

Procédure de mise à jour du Firmware IPS-Firewall

Pour effectuer une mise à jour du Firmware IPS-Firewall, reportez-vous à la procédure suivante :

1. Renseignez les informations nécessaires à la connexion du Firewall Manager au site WEB NETASQ (voir Section « Préférences ») ;

2. Sélectionnez le menu « Maintenance \ Mise à jour WEB \ Chercher des mises à jour de firmware » ;

3. Lorsque le menu apparaît il vous indique s'il existe une version plus récente du firmware actuellement sur le site WEB NETASQ ;

4. Cliquez sur le bouton « Mettre à jour », un dossier de téléchargement est demandé si celui-ci n'a pas été spécifié dans les préférences du Web Update (voir Section « Préférences ») puis le menu de mise à jour des IPS-Firewall apparaît (voir Section « Mise à jour »). Le fichier à renseigner pour la mise à jour du firmware est alors déjà indiqué.

Veillez à la compatibilité de connexion entre la nouvelle suite d'administration et l'IPS-Firewall. En effet NETASQ ne garantit pas la compatibilité entre version majeure.

Chapitre XI

Actions diverses

© Copyright NETASQ 2006

Pour cette section, vous devez avoir franchi les étapes

► Interface graphique,
► Installation, intégration et pré-configuration.

Utilité de la section

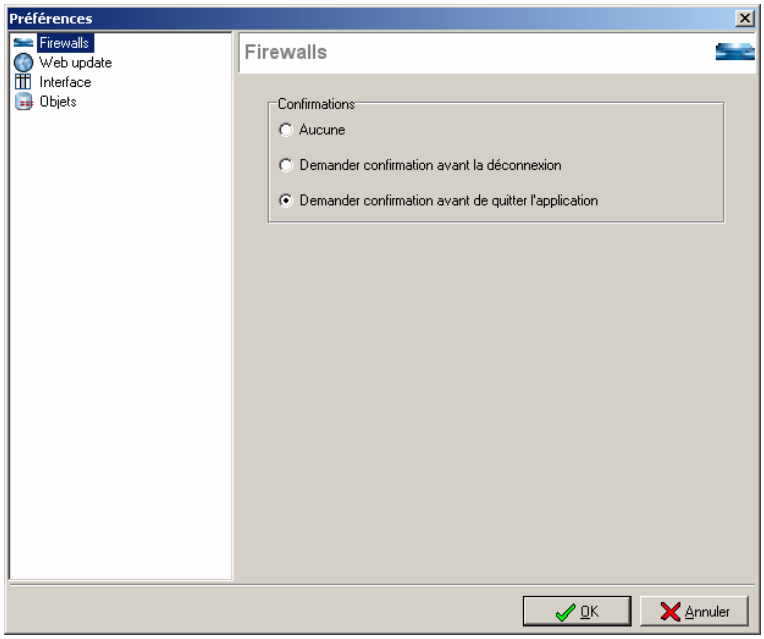
Cette section vous permet de modifier des paramètres divers et généraux de la configuration de l'IPS-Firewall.

© Copyright NETASQ 2006

Les options de gestion de l'application Firewall Manager sont disponibles dans le sous-menu « Fichiers > Préférences ». En cliquant sur ce menu l'écran de configuration des options de l'interface Firewall Manager apparaît.

Le menu de configuration des options d'affichage de l'interface est divisé en deux parties :

► A gauche un arbre présentant les diverses fonctionnalités du menu Préférences,
► A droite les options configurables.



Toute personne ayant accès au poste où se trouve l'interface graphique du Firewall NETASQ, peut accéder à ces fonctionnalités.

Firewalls

Confirmations

Les options de confirmations déterminent la façon dont est terminé l'application Firewall Manager. Il existe trois options de confirmations :

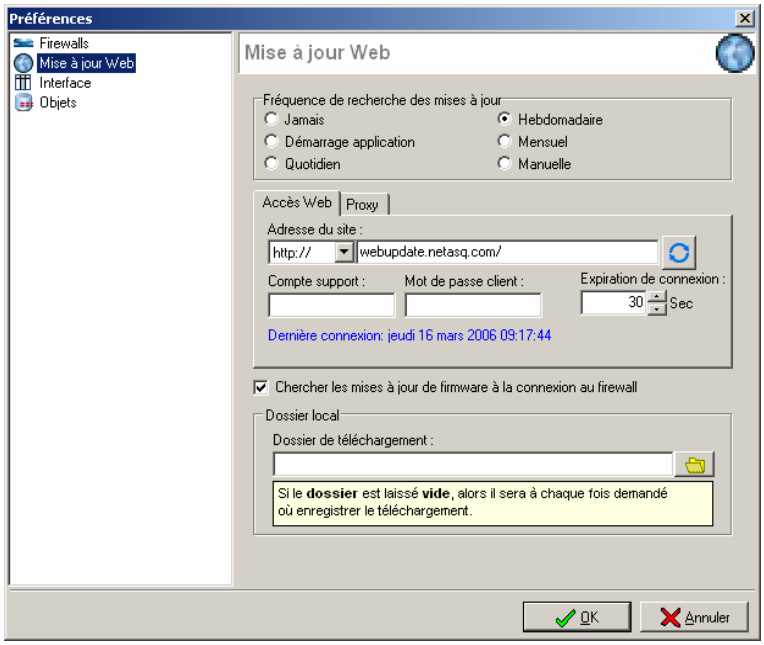
► Aucun : lorsque cette option est sélectionnée, aucune confirmation n'est demandée à la fermeture de l'application Firewall Manager ;

► Demander confirmation avant la déconnexion : un message de confirmation apparaît avant que la connexionn entre le Firewall Manager et l'IPS-Firewall ne soit coupée ;

► Demander confirmation avant de quitter l'application : un message de confirmation apparaît avant la fermeture de l'application Firewall Manager.

© Copyright NETASQ 2006

Web Update



L'IPS-Firewall NETASQ est un produit de sécurité qui évolue pour protéger le réseau, de menaces toujours plus évoluées. Des mises à jour régulières sont nécessaires pour prendre en compte ces différentes évolutions. De plus les logiciels de la suite d'administration doivent être mis à jour pour gérer ces nouvelles fonctionnalités.

Fréquence de recherche des mises à jour

L'intervalle de mise à jour peut être important car lorsque NETASQ publie une nouvelle mise à jour critique, il est préférable que cette mise à jour soit vite repérée. Par défaut cette fréquence de recherche des mises à jour est disposée à « Hebdomadaire » mais il est possible de modifier cet intervalle parmi : « Jamais », « Hebdomadaire », « Mensuel », « Manuelle », « Quotidien » ou « Au démarrage de l'application ».

Par défaut Web Update effectue une recherche de mise à jour de la suite d'administration selon la fréquence sélectionnée. Si l'option « **Chercher les mises à jour de firmware Firewall à la connexion au firewall** » est cochée une recherche automatique de firmware firewall est effectuée. Sinon il n'y a pas de recherche automatique de firmware.

Lorsque la période de référence sélectionnée est écoulée, le Firewall Manager effectue une recherche de mises à jour lors de son démarrage. Si une mise à jour du firmware ou de la suite d'administration est trouvée sur le site WEB NETASQ, une indication est présente sur la page principale du Firewall Manager.

Accès au site WEB

Pour effectuer la recherche des mises à jour sur le site WEB NETASQ, il est nécessaire de spécifier les différentes options suivantes :

► **Adresse du site** : URL en HTTP ou HTTPS permettant de contacter la section du site WEB permettant la recherche des mises à jour. Le bouton « » permet de rappeler l'adresse URL du site qui est spécifiée par défaut ;

► **Compte support** : Compte support obtenu suite à l'enregistrement d'un produit NETASQ sur le site WEB NETASQ. Ce champ est un login ;

► **Mot de passe client** : mot de passe associé au compte support spécifié ci-avant. Par défaut ce mot de passe est le code d'activation indiqué sur l'étiquette située sous le produit NETASQ ;

► **Expiration de connexion** : temps maximum d'attente d'une réponse du serveur WEB NETASQ. Si ce temps est trop faible, le serveur WEB risque de ne pas pouvoir répondre à temps et WEB Update indiquera qu'il n'existe pas de mise à jour alors qu'il en existe une ;

► **Config Proxy** : le bouton « config proxy » permet d'accéder à la configuration d'un proxy pour l'accès de l'application à Internet.

Config Proxy

S'il existe un proxy pour l'accès à Internet sur le réseau, il est indispensable de remplir la configuration du proxy. Sans cette configuration, il sera alors impossible au Firewall Manager de vérifier la présence d'une mise à jour sur le site WEB NETASQ. Les différentes options sont les suivantes :

► **Serveur Proxy** : Nom d'hôte complet ou adresse IP représentant le serveur Proxy ;

► **Port Proxy** : Port à utiliser pour contacter le proxy, par défaut ce port est 3128 ;

► **Identifiant utilisateur** : login de connexion au proxy ;

► **Mot de passe proxy** : mot de passe de connexion au proxy associé au login ;

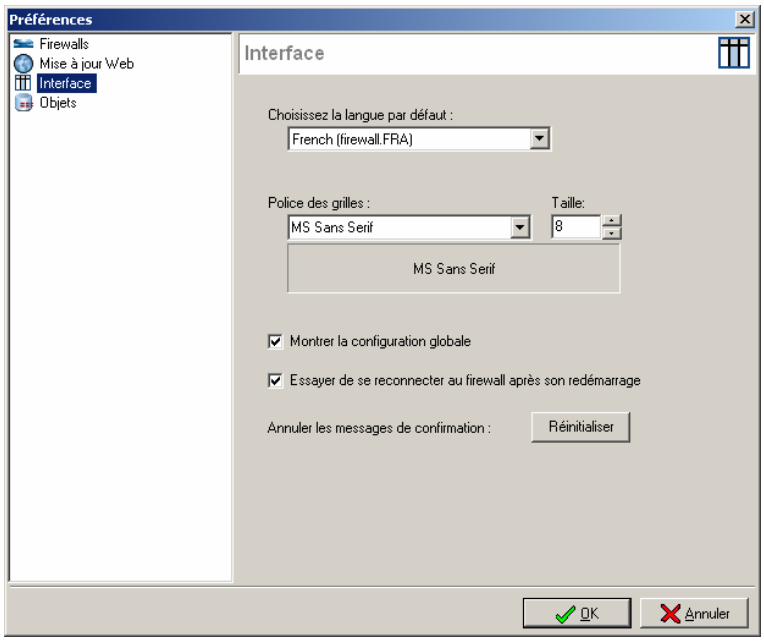
► **Authentification basique** : définit que l'authentification est effective. Si la case n'est plus cochée, il n'y a pas d'authentification même si le proxy la demande ;

► **Config Site Web** : le bouton « config site web » permet de retourner à la configuration des options pour l'accès au serveur WEB NETASQ.

Dossier de téléchargement

Si une mise à jour du firmware ou de l'application Firewall Manager est découverte sur le serveur WEB NETASQ elle devra être téléchargée dans le « Dossier de téléchargement ». Si le champ n'est pas renseigné, le dossier de téléchargement sera demandé à chaque téléchargement.

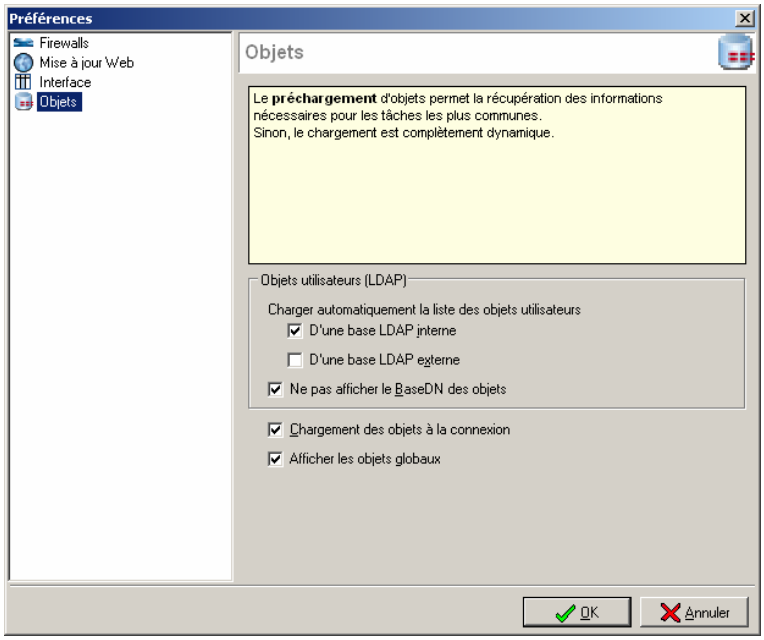
Interface



Les différentes options de l'interface sont présentées dans le tableau suivant :

Choisissez la langue par défaut	Cette option vous permet de choisir la langue dans laquelle apparaissent les menus de l'interface graphique. Attention, une fois la langue choisie, vous devez redémarrer l'interface pour prendre en compte la modification. Le choix « Sélection automatique » permet d'utiliser la langue utilisée par le système d'exploitation « Windows ».
Police des grilles	Polices et tailles des informations qui seront affichées dans les grilles de configuration du Firewall Manager (Exemple : règles de filtrage).
Montrer la configuration globale	Par défaut les menus de la configuration globale sont cachés car il s'agit d'une option de configuration très avancée. En cochant cette option les menus de la configuration globale apparaîssent dans la barre de menus situées en haut de l'interface : « Configuration globale ».
Essayer de se reconnecter au firewall après son redémarrage	Lors du redémarrage d'un appliance UTM, il est possible de configurer le Firewall Manager pour que celui-ci se reconnecte automatiquement à l'appliance sans avoir à surveiller son redémarrage effectif. Pour plus d'informations sur les effets de cette option, dirigez vous dans la section « Redémarrage du firewall ».
Annuler les messages de confirmation	Certains menus de configuration demandent la confirmation de l'abandon des modifications avant de quitter un menu. Ces messages peuvent être masqués. Le bouton « Réinitialiser » permet la remise à zéro des messages de confirmation masqués.

Objets

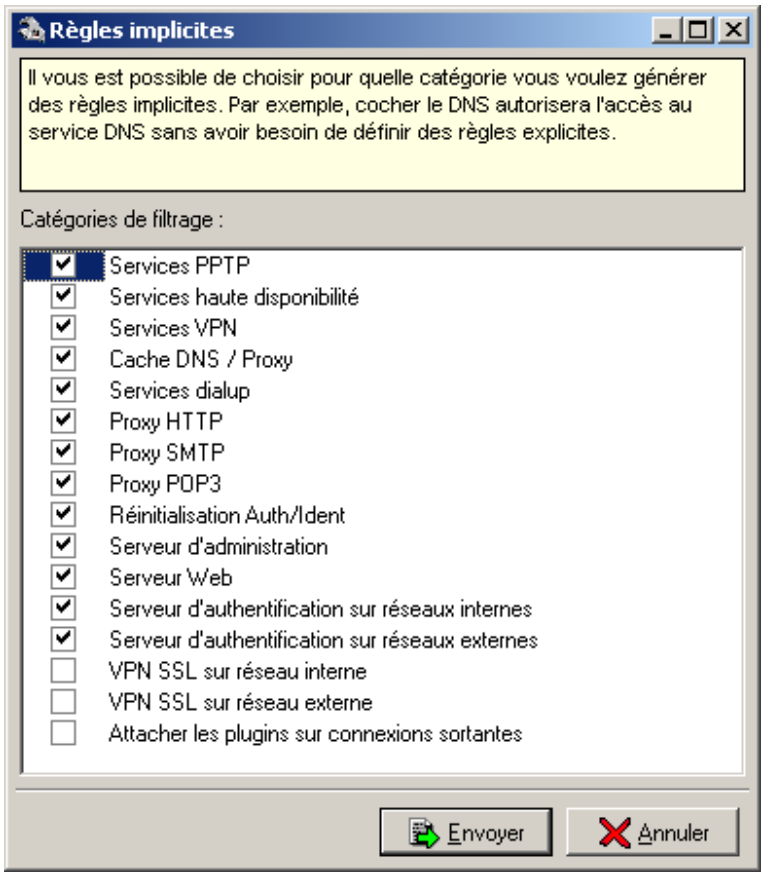


Les différentes options de traitement des objets sont présentées dans le tableau suivant :

Charger	Par défaut, lorsque la base LDAP est chargée entièrement dans

automatiquement la liste des objets utilisateurs	la configuration des objets, le Firewall Manager affiche un message d'avertissement, car dans certains cas, la base LDAP peut s'avérer conséquente et le chargement est alors très long. En cochant sur l'option « Base LDAP interne », ce message d'avertissement est masqué dans le cas d'une base LDAP interne. En cochant sur l'option « Base LDAP externe », ce message d'avertissement est masqué dans le cas d'une base LDAP externe.
Ne pas afficher le BaseDN des objets	Les utilisateurs stockés dans les bases d'utilisateurs utilisées par les appliances NETASQ (internes ou externes) sont identifiés par leur nom (appelé CN ou Common Name) et l'organisation à laquelle ils appartiennent (appelé BaseDN). Ce BaseDN est identique à tous les utilisateurs de la base et reprend les champs O (Nom de la société) et DC (Pays) demandés dans la construction des bases LDAP. Cocher l'option « Ne pas afficher le BaseDN des objets » simplifie l'affichage des objets utilisateurs et groupes d'utilisateurs en masquant la partie « organisation ».
Chargement des objets à la connexion	Cette option permet un chargement anticipé de certaines informations nécessaires à la réalisation de tâches basiques.
Afficher les objets globaux	Permet l'affichage des objets globaux.

En sélectionnant « Règles implicites » dans le menu « Politique » de l'arborescence de l'interface graphique, l'écran de configuration des règles implicites s'affiche alors.


Règles implicites
Il vous est possible de choisir pour quelle catégorie vous voulez générer des règles implicites. Par exemple, cocher le DNS autorisera l'accès au service DNS sans avoir besoin de définir des règles explicites.
Catégories de filtrage :
Services PPTP
Services haute disponibilité
Services VPN
Cache DNS / Proxy
Services dialup
Proxy HTTP
Proxy SMTP
Proxy POP3
Réinitialisation Auth/Ident
Serveur d'administration
Serveur Web
Serveur d'authentification sur réseaux internes
Serveur d'authentification sur réseaux externes
VPN SSL sur réseau interne
VPN SSL sur réseau externe
Attacher les plugins sur connexions sortantes
Envoyer
Annuler

Dans cet écran on vous informe qu'il est possible de générer automatiquement certaines règles liées à l'utilisation des services du firewall. Si vous cochez un service, le firewall crée de lui-même les règles d'utilisation de ce service.

► Services PPTP : pour les tunnels sécurisés en PPTP,

► Services Haute Disponibilité : pour la haute disponibilité,

► Services VPN : pour les tunnels VPN,

► Cache DNS/Proxy : pour le cache DNS,

► Services Dialup : pour les connexions distantes,

► Proxy HTTP : pour le proxy HTTP,

► Proxy SMTP : pour le proxy SMTP,

► Proxy POP3 : pour le proxy POP3,

► Réinitialisation Auth/Ident : pour la vérification de l'existence d'un utilisateur (FTP par exemple),

► Serveur d'administration : autorise l'accès avec l'interface graphique à partir d'une machine située sur les réseaux internes. Cette option crée une règle implicite au niveau du firewall. Si cette option est désélectionnée, il faudra créer une règle explicite, dans les

© Copyright NETASQ 2006

règles de filtrage, pour autoriser la connexion au Firewall via le Firewall Manager (service Firewall_srv, port 1300),

► Serveur WEB : autorise l'accès àl'EZADMIN présent sur l'IPS-Firewall.

► Serveur d'authentification sur les réseaux internes : autorise l'accès au service d'authentification pour les utilisateurs des réseaux internes. Ce service utilise les ports 443 (https) et 1200,

► Serveur d'authentification sur les réseaux externes : autorise l'accès au service d'authentification pour les utilisateurs des réseaux externes. Ce service utilise les ports 443 (https) et 1200,

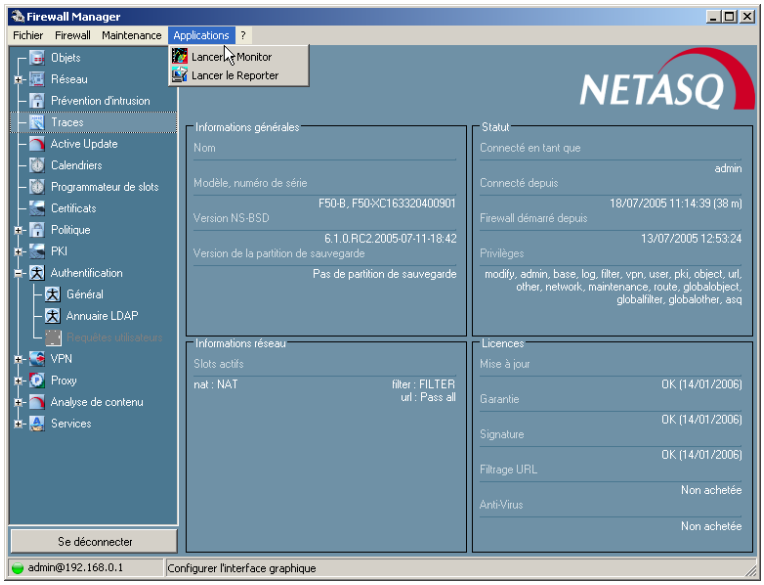
► XVPN sur les réseaux internes : autorise l'accès au VPN SSL pour des utilisateurs des réseaux internes (les interfaces Ethernet et VLAN possédant l'attribut « protégée »)

► XPVN sur les réseaux externes : autorise l'accès au VPN SSL pour des utilisateurs des réseaux externes (les interfaces Ethernet et VLAN ne possédant pas l'attribut « protégée » et les interfaces de type Dialup).

► Attacher les plugins sur les connexions sortantes : lorsque cette option est cochée, lors d'une connexion sortante, le plugin correspondant à cette connexion sera automatiquement attaché.

Le menu Applications se décompose en deux sous-menu :

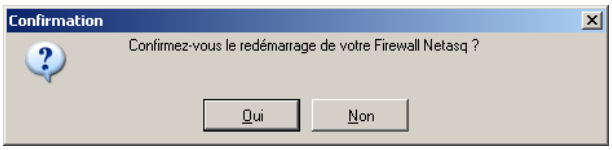
- ► Lancez le Moniteur,
- ► Lancez le Reporter.



Ces deux sous-menus permettent l'ouverture des logiciels Monitor et Reporter de la suite d'administration NETASQ au moyen du Firewall Manager, utiliser les deux raccourcis procurent l'avantage de ne pas devoir se ré authentifier sur le deux applications. L'authentification réalisée sur le Firewall Manager est réalisée par les deux applications.

© Copyright NETASQ 2006

Pour redémarrer le Firewall NETASQ, allez dans le sous-menu « Firewall > Redémarrer le firewall ». Une boîte de dialogue vous informant du redémarrage de l'IPS-Firewall s'affiche alors.



Cliquez sur le bouton « Oui » et le Firewall NETASQ redémarre à distance.

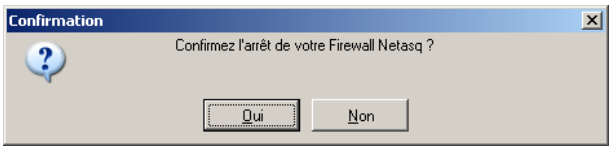
Le redémarrage d'un IPS-Firewall NETASQ implique le blocage systématique de tout paquet et donc detoute communication transitant par le Firewall NETASQ, ainsi qu'une déconnexion du logiciel de configuration sous Windows (Ceci est visible dans l'écran principal par le passage à la couleur rouge du voyant d'état).

Vous devrez vous connecter à nouveau pour pouvoir continuer la configuration de votre Firewall NETASQ.

Une fois que le Firewall NETASQ a redémarré (une minute après l'envoi de la commande), celui-ci réactive les règles de sécurité et de log en vigueur avant son redémarrage.

© Copyright NETASQ 2006

Pour arrêter le Firewall NETASQ à distance, allez dans le sous-menu « Firewall > Arrêter le firewall ». Une boîte de dialogue vous informant de l'arrêt de l'IPS-Firewall s'affiche alors.



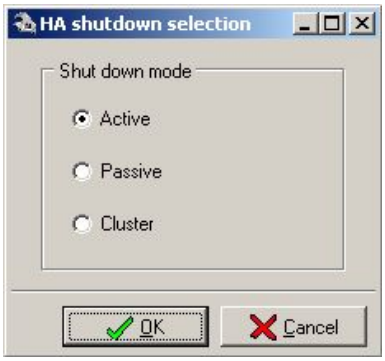
L'arrêt du Firewall NETASQ implique le blocage systématique de tout paquet transitant par le Firewall, ainsi qu'une déconnexion du logiciel de configuration sous Windows (Ceci est visible dans l'écran principal par le passage à la couleur rouge du voyant d'état). Vous devez vous connecter à nouveau pour pouvoir continuer la configuration de votre Firewall NETASQ. Ceci arrête le Firewall NETASQ à distance. Le firewall est arrêté une fois que le voyant "Power" est éteint. Les voyants d'activité des cartes réseaux (IN, OUT et DMZ) restent en fonctionnement. Vous pouvez aussi, sur certains modèles, éteindre le boîtier grâce au bouton prévu à cet effet en façade du produit.

Il est fortement conseillé d'attendre l'extinction du voyant « Power » après une demande d'arrêt manuelle ou à distance, avant de couper l'alimentation du Firewall.

Une coupure trop rapide peut entraîner des problèmes d'écriture sur le disque du Firewall et provoquer des erreurs matérielles.

Cas de la haute disponibilité

Lorsque votre firewall fait partie d'un cluster (haute disponibilité avec un deuxième firewall), une boîte de dialogue s'affiche alors, grâce à cet écran vous pouvez choisir de stopper le firewall actif, le firewall passif ou les deux.



© Copyright NETASQ 2006

Introduction

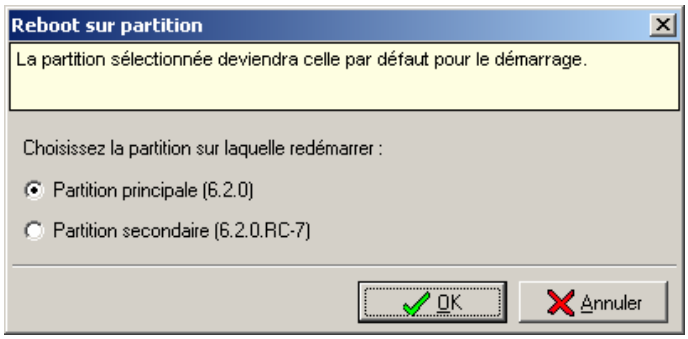
Les appliances UTM NETASQ qui possèdent un disque dur (soit les produits NETASQ à partir du F200) permettent la sauvegarde de leur système principal sur une partition de backup. Ainsi lorsque leur système principal est corrompu ou la configuration effectuée ne permet pas la reprise en main du boîtier, il est possible de démarrer le produit NETASQ sur cette partition de backup, restée quant à elle, « propre ».

Pour démarrer un appliance UTM NETASQ sur sa partition de backup, il existe deux possibilités. La première nécessite une connexion en mode console au boitier (lien série) et n'est pas évoquée dans cette section. De plus la méthode en mode console ne permet qu'un démarrage manuel (action systématique de l'administrateur au moment du démarrage) sur la partition de backup.

Dans un deuxième temps, le menu « Maintenance > Partition de démarrage » du logiciel Firewall Manager, permet quant à lui la définition de la partition de démarrage par défaut de l'appliance UTM. Ainsi, sans connexion en mode console (lien série) et à distance, il est possible de redémarrer le boitier sur sa partition de backup et cela de manière automatique et systématique.

Configuration

Cliquez sur le sous-menu « Maintenance > Partition de démarrage » est l'écran de configuration de la partition de démarrage apparaît.


Reboot sur partition
La partition sélectionnée deviendra celle par défaut pour le démarrage.
Choisissez la partition sur laquelle redémarrer :
Partition principale (6.2.0)
Partition secondaire (6.2.0.RC-7)
OK
Annuler

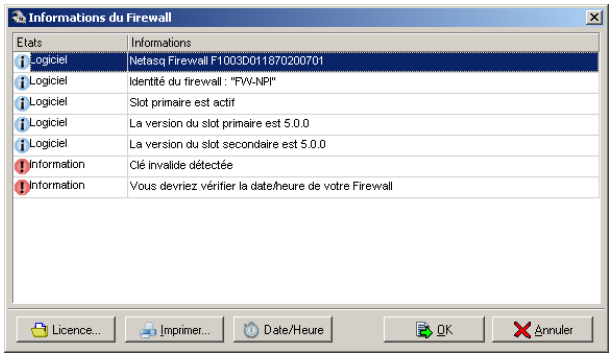
Ce simple écran indique les deux partitions détectées sur le disque dur de l'appliance et la version disponible sur cette partition. Pour définir la partition de démarrage par défaut de l'appliance, choisissez simplement la partition parmi les partitions proposées et cliquez sur « OK » pour valider les changements.

© Copyright NETASQ 2006

Chaque Firewall possède une licence qui définit l'ensemble des fonctionnalités disponibles pour votre Firewall. Cette clé vous permet d'activer certaines options du Firewall (filtrage d'URL, chiffrement VPN fort, mises à jour ...). Cette clé peut être récupérée sur le site WEB NETASQ (www.netasq.com).

Première connexion

Lors de votre première connexion, le firewall ne contient aucune licence. Sans elle, il est inutilisable. L'écran de configuration de la licence apparaît alors.



Si, à la réception de votre firewall, aucun message concernant la licence n'apparaît, c'est que NETASQ a installé une licence temporaire dans votre produit. Cette licence correspond à la licence minimale du produit NETASQ (aucune option n'est activée). De plus si un incident survient alors que la licence temporaire est toujours installée sur votre produit, vous ne serez pas couvert par la garantie. Ainsi même si votre firewall fonctionne temporairement, NETASQ vous conseille de télécharger au plus vite votre licence définitive avant l'expiration de cette licence temporaire.

Le bouton « Licence » vous permet d'insérer votre licence préalablement récupérée sur le site web NETASQ et ainsi activer la configuration de votre firewall

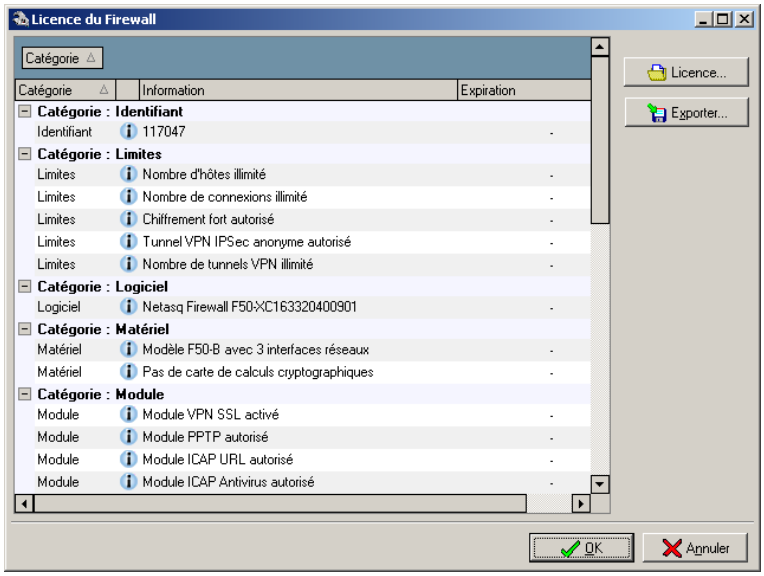
De plus comme il l'est conseillé vous pouvez vérifier la date et l'heure de votre firewall par le bouton « Date/heure ».

Enfin vous pouvez imprimer les informations relatives à votre firewall, en cliquant sur le bouton « Imprimer ».

La licence de votre firewall et sa mise à jour

Ces renseignements sont accessibles par le menu « Firewall > Informations ». L'écran de configuration de la licence vous donne la version de votre Firewall, des informations sur le matériel et les différentes options avec leur date d'expiration s'il y en a une.

© Copyright NETASQ 2006



Le Firewall NETASQ est livré par défaut avec l'ensemble de ses fonctionnalités. Cependant, certaines fonctionnalités (filtrage URL, haute disponibilité...) sont optionnelles et ne sont pas activées. D'autre part certaines options, comme la mise à jour, sont limitées dans le temps. Si la date d'expiration est dépassée, certaines options sont désactivées sur le Firewall.

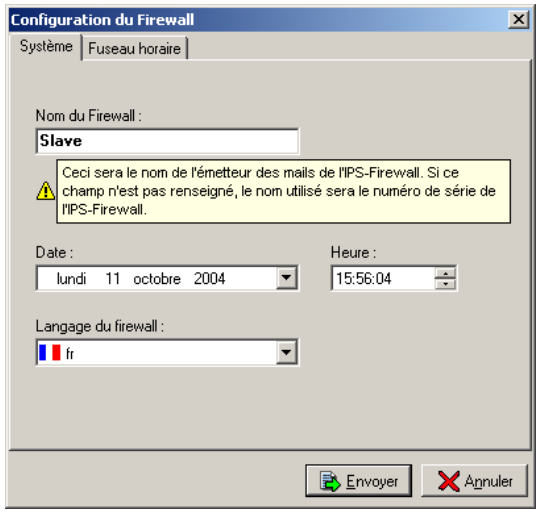
Si vous choisissez d'utiliser de nouvelles fonctionnalités ou renouveler certaines options, veuillez contacter votre revendeur. Une nouvelle clé sera alors disponible sur le site web de NETASQ. Entrez cette clé avec le bouton "Mettre à jour la licence" situé en bas à gauche puis Validez en envoyant au Firewall. Les informations concernant votre Firewall sont modifiées et les nouvelles options sont activées sur le Firewall.

Vous pouvez imprimer les informations relatives à votre firewall, en cliquant sur le bouton « Imprimer ».

© Copyright NETASQ 2006

Pour modifier les paramètres du Firewall NETASQ allez dans le sous menu « Firewall > Configuration système ». L'écran de configuration système est divisé en deux onglets :

► L'onglet Système,
► L'onglet Fuseau horaire.



Onglet Système

L'onglet système permet la modification des paramètres suivants :

► Nom du firewall (ce nom est utilisé dans les mails d'alarmes envoyés à l'administrateur et est affiché sur la fenêtre principale du Firewall Manager). Ce nom peut-être quelconque,
► Date. Choisissez la date sur le calendrier,
► Heure,
► Langage du firewall (type de clavier supporté par le Firewall).

La date et l'heure auxquelles votre Firewall NETASQ est réglé sont importantes : elles vous permettent de situer dans le temps un événement enregistré dans le fichier log. Elles servent également à la programmation horaire des configurations.

A chaque ouverture de cette boîte de dialogue, le logiciel de configuration à distance vous indique l'heure et la date actuellement paramétrées sur le Firewall NETASQ.

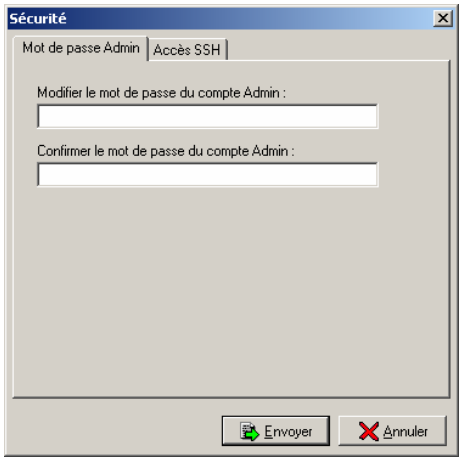
Onglet Fuseau horaire

L'onglet Fuseau horaire vous permet de configurer la plage horaire de votre firewall.

Attention un changement de fuseau horaire entraîne un reboot du firewall.

© Copyright NETASQ 2006

Pour modifier les paramètres de sécurité du Firewall NETASQ allez dans le sous-menu « Firewall > Sécurité ».



Ce menu est constitué de deux onglets :

Mot de passe Admin	Permet la modification du mot de passe du compte super-administrateur, le compte « admin ».
Accès SSH	Configuration de l'accès à l'appliance NETASQ via un client SSH en mode console.

Mot de passe Admin

Les champs "Modifier le mot de passe de la clé privée adm" et "Confirmer le mot de passe de la clé privée admin" vous permettent de modifier le mot de passe utilisé pour vous connecter en SSH au firewall. Ce mot de passe correspond au mot de passe du compte "admin". Si vous changez le mot de passe, vous devrez aussi utiliser ce nouveau mot de passe pour vous connecter via l'interface graphique, sous le compte "admin".

Accès SSH

Le firewall possède un serveur SSH (version 2) intégré. Ce serveur vous permet, via un client SSH, d'accéder au firewall en mode console de façon totalement sécurisée. La configuration du serveur peut se réaliser à partir de cet onglet. Les communications entre un client et un serveur SSH sont chiffrées et authentifiées afin d'assurer un maximum de sécurité durant la configuration. Pour activer le serveur, cochez la case "Activer l'accès SSH au firewall". Si cette case n'est pas cochée, il sera impossible de vous connecter à distance en mode console.

Vous pouvez exporter la clé publique du firewall et la clé privée de l'administrateur, afin de les installer sur la machine intégrant le client SSH, grâce aux boutons appropriés. Le format d'export de la clé privée de l'admin est celui d'OpenSSH, incompatible avec SSH.COM.

SSH fonctionne avec certificats. Toutefois vous pouvez toujours activer « Activer l'accès par mot de passe » pour utiliser un accès login/password mais cette option n'est pas recommandée.

Par défaut, le filtrage du firewall bloque la connexion sur le port 22 (SSH) du Firewall. Il est donc nécessaire de mettre en place une règle de filtrage pour autoriser cette communication.

© Copyright NETASQ 2006

Introduction

La configuration de l'IPS-Firewall contient des informations très sensibles. Ces informations révèlent l'activité du réseau et la manière de contourner les mécanismes de protection de ce réseau. Pour protéger ces données sensibles, il est possible d'utiliser les fonctionnalités de chiffrement des IPS-Firewalls sur les fichiers de configuration de l'IPS-Firewall lui-même.

Les fichiers de configuration chiffrés ne pouvant être déchiffrés qu'au moyen d'un secret détenu par l'IPS-Firewall et l'administrateur, ce dernier se protège contre le vol et l'utilisation illicite de son IPS-Firewall. En effet sans déchiffrement des fichiers, l'IPS-Firewall est inutilisable.

Principe de fonctionnement

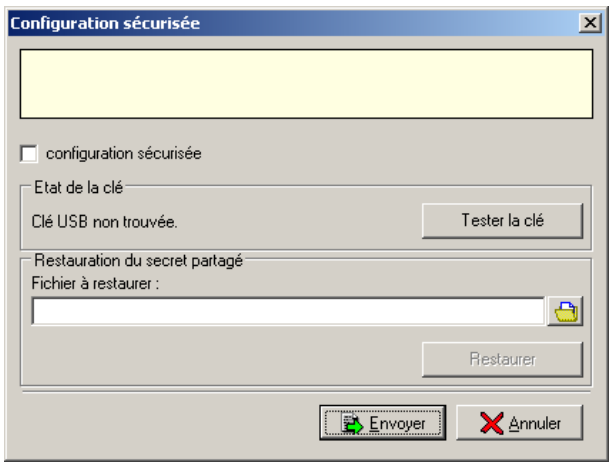
Pour mettre en place cette technologie, NETASQ propose l'utilisation de clés USB qui contiendront les secrets échangés. Sans cette clé, il est impossible de démarrer l'IPS-Firewall. Une fois la configuration chargée en mémoire, la clé USB peut être retirée pour préserver la confidentialité des fichiers de configuration. Au prochain démarrage, la clé est de nouveau indispensable.

NETASQ a qualifié des clés USB compatibles avec cette fonctionnalité. Seuls les clés USB qualifiées et distribuées par NETASQ sont donc supportées pour cette fonctionnalité.

Cette fonctionnalité n'est disponible que pour les produits possédant un port USB effectivement fonctionnel.

Configuration

L'activation des fonctionnalités de configuration sécurisée est réalisée dans le sous-menu « Configuration sécurisée » du menu « Firewall » de la barre de menu de l'interface graphique Firewall manager.



Les différentes options de la configuration sécurisée sont présentées dans le tableau suivant :

Configuration sécurisée	Bouton d'activation de la configuration sécurisée. Une fois activée, les fichiers de configuration de l'IPS-Firewall sont chiffrés. Il est alors indispenble de posséder la clé USB contenant le secret échangé avec l'IPS-Firewall pour déchiffrer sa configuration.
Etat de la clé	Valeur informative remontée par l'IPS-Firewall indiquant l'état actuel de la clé qui servira à sotcker le secret de déchiffrement. Il existe trois états différents : ► Clé USB non trouvée : la clé n'est pas insérée dans le port USB de l'IPS-Firewall ou pas formatté selon son format de fichiers ; ► Clé USB non initialisée : la clé est détectée mais elle ne contient pas de secret de déchiffrement de la configuration de l'IPS-Firewall ; ► Clé USB initialisée : la clé est détectée et elle contient un secret de déchiffrement de la configuration de l'IPS-Firewall.
Test de la clé	Avant l'affichage du menu « Configuration sécurisée », le Firewall Manager vérifie l'état de la clé. Le bouton « Test de la clé » permet l'actualisation des informations affichées. Si une clé USB est inséré après l'affichage du menu « Configuration sécurisée », cliquez sur le bouton « Test de la clé » pour actualiser les informations d'état de la clé.
Restauration du secret partagé.	Si le secret contenu par la clé ou la clé elle-même est défectueuse, il est alors possible de restaurer cette sauvegarde sur la même clé ou sur une autre clé vierge.
Envoyer	Activation de la configuration sécurisée. Avant la fermeture du menu, il est demandé de spécifier un chemin pour la sauvegarde de la clé de déchiffrement insérée dans la clé USB.
Annuler	Annule le paramétrage modifié de la configuration sécurisée.

Les fichiers de configuration chiffrés

Afin de faciliter la configuration, l'activation et l'utilisation de cette fonctionnalité, le Firewall Manager ne permet pas le choix des fichiers de la configuration qui seront chiffrés. Par défaut les fichiers chiffrés par la configuration sécurisée sont :

► Les clés pré-partagées de la configuation VPN ;
► La configuration de l'annuaire LDAP ;
► La configuration de l'authentification ;
► Le fichier Keytab de la configuration SPNEGO ;
► La clé privée de l'autorité de certification de la PKI ;
► La configuration de la PKI ;
► Les certificats signés par l'autorité de certification de la PKI.

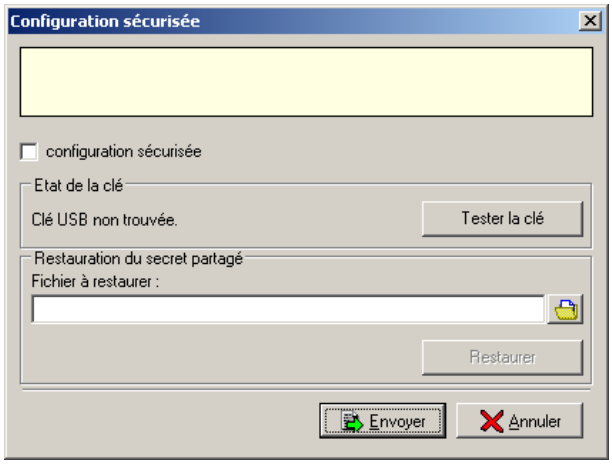
Utilisation

L'utilisation de la fonctionnalité de chiffrement de la configuration n'est possible qu'avec les produits possédant un port USB et l'administrateur doit posséder d'une clé USB compatible. Contactez votre partenaire pour obtenir cette clé USB.

Une fois la configuration sécurisée activée, la clé USB contenant le secret est indispensable au démarrage du produit. L'administrateur retire cette clé après le démarrage de l'IPS-Firewall ainsi la configuration de l'appliance est sécurisée.

Pour activer la configuration sécurisée, reportez-vous à la procédure suivante :

1. Sélectionnez le menu de configuration « Firewall\Configuration Sécurisée », l'écran de la configuration sécurisée apparaît ;



2. Connectez la clé USB ;
3. Cliquez sur « Tester la clé », l'état de la clé doit être alors « Clé USB non initilalisée » ;
4. Cochez l'option « Configuration sécurisée » ;
5. Cliquez sur « Envoyer » pour activer la configuration sécurisée ;
6. La clé est initialisée, les fichiers de configuration de l'IPS-Firewall sont chiffrés et un chemin de copie du fichier de sauvegarde est demandé.

Restaurer une clé défectueuse ou création d'une clé de sauvegarde

Lors de la génération de l'initialisation de la clé USB contenant le secret partagé avec l'IPS-Firewall, le Firewall Manager effectue une sauvegarde de ce secret. Il est ainsi possible de réaliser des opérations de sauvegarde sur les clés USB.

Pour restaurer une clé USB, reportez-vous à la procédure suivante :

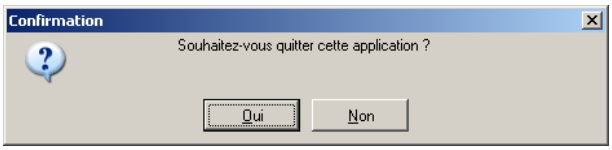
1. Sélectionnez le menu de configuration « Firewall\Configuration Sécurisée », l'écran de la configuration sécurisée apparaît ;
2. Connectez la clé USB ;
3. L'état de la clé peut être « Clé non initialisée » ou « Clé initialisée » suivant la dégradation de la clé ;
4. L'option « Configuration sécurisée » est normalement déjà cochée ;
5. Sélectionnez le fichier de sauvegarde à restaurer en cliquant sur l'icône ;
6. Cliquez sur « Restaurer » pour restaurer la clé USB ;
7. Cliquez sur « Envoyer » pour terminer la restauration.

Pour créer une clé USB de sauvegarde, reportez-vous à la procédure suivante :

1. Sélectionnez le menu de configuration « Firewall\Configuration Sécurisée », l'écran de la configuration sécurisée apparaît ;
2. Connectez la clé USB vierge ;
3. Cliquez sur « Tester la clé », l'état de la clé doit être alors « Clé USB non initilalisée » ;
4. L'option « Configuration sécurisée » est normalement déjà cochée ;
5. Sélectionnez le fichier de sauvegarde à restaurer en cliquant sur l'icône ;
6. Cliquez sur « Restaurer » pour restaurer la clé USB ;
7. Cliquez sur « Envoyer » pour terminer la création de la clé USB de sauvegarde.

© Copyright NETASQ 2006

Lors de la fermeture de l'application une boîte de dialogue vous demande de confirmer l'action (suivant les options configurées dans le menu « Fichier >option ») :



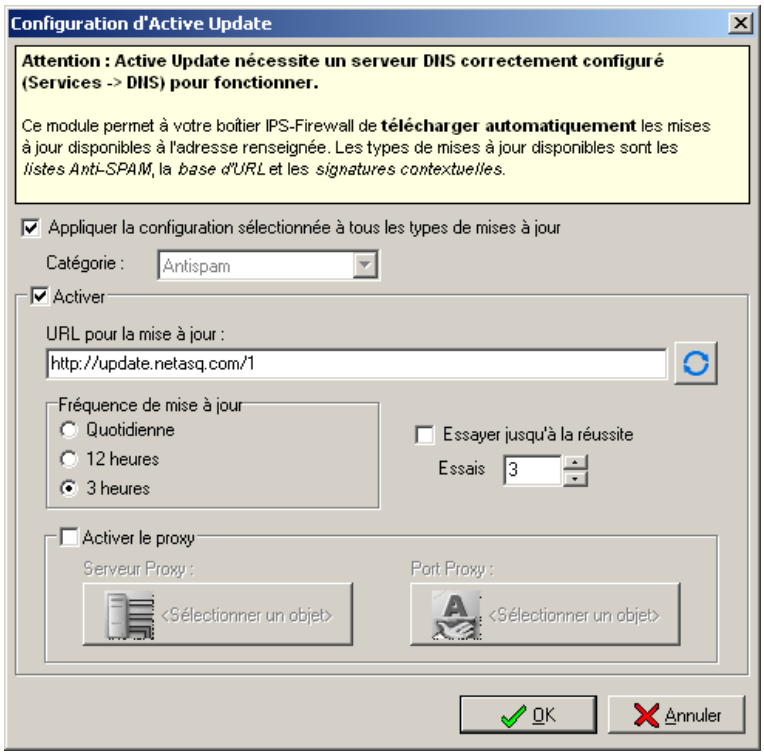
► L'annulation provoque le retour à l'écran principal, sans conséquence pour la suite de l'exécution du programme.

► La confirmation quitte l'application.

Cette boîte est également affichée quand vous quittez l'application en cliquant sur en haut à droite de la fenêtre Windows.

© Copyright NETASQ 2006

Introduction


Configuration d'Active Update
Attention : Active Update nécessite un serveur DNS correctement configuré (Services -> DNS) pour fonctionner.
Ce module permet à votre boîtier IPS-Firewall de télécharger automatiquement les mises à jour disponibles à l'adresse renseignée. Les types de mises à jour disponibles sont les listes Anti-SPAM, la base d'URL et les signatures contextuelles.
Appliquer la configuration sélectionnée à tous les types de mises à jour
Catégorie :
Antispam
Activer
URL pour la mise à jour :
http://update.netasq.com/1
Fréquence de mise à jour
Quotidienne
12 heures
3 heures
Essayer jusqu'à la réussite
Essais
3
Activer le proxy
Serveur Proxy :
<Sélectionner un objet>
Port Proxy :
<Sélectionner un objet>
OK
Annuler

Le module Active Update des IPS-Firewalls permet la mise à jour de la base antivirale des antivirus, les signatures contextuelles ASQ, la liste des serveurs antispam et les URLs utilisées pour le filtrage URL dynamique.

© Copyright NETASQ 2006

Fonctionnement

Pour chaque type de données pouvant être mises à jour (ou toutes d'un coup si l'option « Appliquer la configuration sélectionnée à tous les types de mises à jour » est cochée) il est nécessaire de configurer les paramètres expliqués dans le tableau suivant :

Activer	Activation de la mise à jour via l'Active Update pour le type de mise à jour sélectionné.
URL de mise à jour	Chemin à spécifier pour la réalisation de la mise à jour par l'Active Update.
Fréquence	Fréquence de mise à jour des listes d'URL dynamique, des signatures contextuelles ASQ et de la configuration de l'antispam. Choisir la fréquence parmi : « Journalier », « toutes les 12 heures », « toutes les 6 heures ».
Ressayer jusqu'au succès	Cette option vous permet de spécifier que l'Active Update essaiera de réaliser la mise à jour jusqu'à son succès. Le champ « Tentatives » situé sous l'option « Ressayer jusqu'au succès » permet de spécifier un nombre de tentative avant l'abandon de la mise à jour. Les deux options sont incompatibles.

Activation du proxy

Lorsque l'IPS-Firewall n'est pas directement connecté à Internet mais par l'intermédiaire d'un proxy, il faut configurer ce proxy pour que la mise à jour puisse être effectuée. La configuration de ce proxy se réalise en choisissant dans la base d'objet un serveur et le port sur lequel il doit être contacté.

Chapitre XII

NETASQ Syslog

© Copyright NETASQ 2006

L'interface graphique d'administration des firewalls NETASQ est complétée par un utilitaire de récupération des traces. Cet utilitaire baptisé NETASQ SYSLOG vous permet de récupérer les traces générées par le firewall pour les exploiter ensuite.

Intérêt du NETASQ SYSLOG

Certains produits NETASQ ne possèdent pas de disque dur. Le stockage des traces n'est alors pas possible en local sur le firewall. Il faut nécessairement rediriger les traces vers un équipement externe.

En installant le NETASQ SYSLOG sur la machine d'administration, les traces sont récupérées puis stockées sur cette machine.

© Copyright NETASQ 2006

Attention : Si vous tentez d'installer une nouvelle version du NETASQ SYSLOG et qu'une version antérieure a déjà été installée en tant que service, vous devez impérativement arrêter le service et le désinstaller (via la procédure en ligne de commandes, voir section Service SYSLOG).

Le cas contraire peut entraîner une possible corruption de la base de registre et de la gestion des installations Windows.

La machine d'administration doit être protégée correctement car les traces sont stockées en clair sur la machine d'administration (comme le sont les logs d'un SYSLOG classique). La clef de chiffrement des flux entre le NETASQ SYSLOG et le firewall est aussi stockée en clair sur la machine. L'accès à la machine d'administration doit donc être fortement restreint et toute session Windows doit être verrouillée lorsqu'elle n'est pas utilisée.

© Copyright NETASQ 2006

Section A

Installation

© Copyright NETASQ 2006

Etant donné que le logiciel doit être installé sur le même poste que l'interface d'administration du firewall, il demande les mêmes pré-requis matériels et logiciels que le firewall Manager.

Procédure d'installation

1. Récupérez le fichier d'installation de l'Administration Suite sur le site WEB NETASQ ou sur le CD-Rom livré avec le firewall. Executez ce fichier, lorsque le choix vous sera proposé, choisissez l'installation complète (dans ce cas, tous les logiciels de l'Administration Suite seront réinstallés) ou choisissez l'installation personnalisée puis sélectionnez le NETASQ Syslog dans la liste des applications.

2. Exécutez ce fichier sur la machine d'administration afin de lancer l'installation.

3. L'installation se déroule comme une installation standard de logiciel.

Par défaut, le NETASQ SYSLOG se lancera à chaque ouverture de session sous Windows NT et 2000, à chaque reboot sous Windows 95 et 98 (le NETASQ SYSLOG se comporte alors comme un service). Vous avez la possibilité, sous Windows NT et Windows 2000, d'installer le NETASQ SYSLOG comme service. (voir la section Service Syslog).

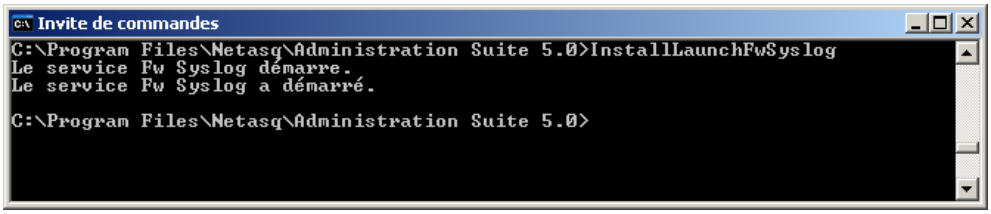
Attention : Si vous tentez d'installer une nouvelle version du NETASQ SYSLOG et qu'une version antérieure a déjà été installée en tant que service, vous devez impérativement arrêter le service et le désinstaller (via la procédure en ligne de commandes, voir section Service SYSLOG). Le cas contraire peut entraîner une possible corruption de la base de registre et de la gestion des installations Windows.

© Copyright NETASQ 2006

Le NETASQ Syslog peut être installé en tant que service. Ce mode procure l'avantage de tourner de façon totalement transparente pour l'utilisateur (en tâche de fond). De plus, le service SYSLOG continue de fonctionner même sans ouverture de session Windows.

Les procédures qui suivent ne concernent que les plate-formes Windows NT, XP ou 2000. Sous Windows 95 et 98, le NETASQ SYSLOG est installé, par défaut, comme un service qui se lance à chaque redémarrage de la machine (même sans ouverture de session).

Procédure d'installation du service


Invite de commandes
C:\Program Files\Netasq\Administration Suite 5.0>InstallLaunchFwSyslog
Le service Fw Syslog démarre.
Le service Fw Syslog a démarré.
C:\Program Files\Netasq\Administration Suite 5.0>

Le service SYSLOG peut être installé simplement en lançant l'exécutable « Lancer le Syslog » présent dans le menu :

« Démarrer>Programmes>Netasq>Administration Suite 5.0>Services »

Sinon, la procédure complète est la suivante :

1. Ouvrez une invite de commandes DOS,

2. Placez-vous sur le répertoire NETASQ de votre disque dur, (en principe : c:\Program Files\netasq\Administration Suite x.x),

3. Tapez la commande d'installation suivante : InstallLaunchFwSyslog, le service démarre automatiquement.

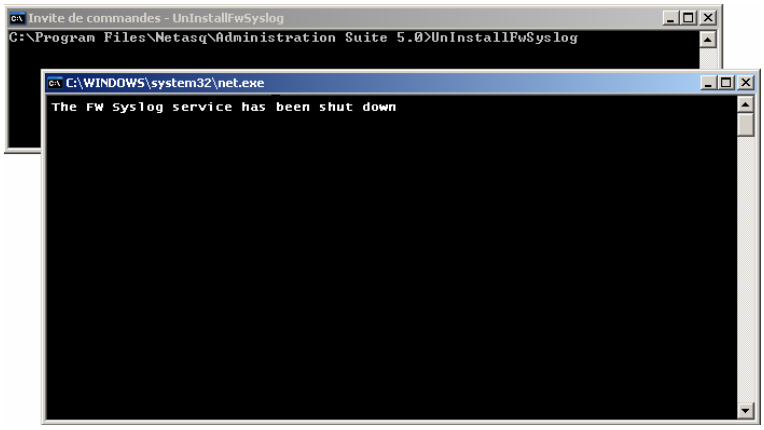
Il est conseillé de redémarrer le poste après installation du service SYSLOG.

Une fois installé, le service sera redémarré à chaque reboot même si aucune session n'est ouverte.

Attention : N'oubliez pas de modifier les options du NETASQ SYSLOG (voir la section Configuration) afin de ne pas le lancer automatiquement à chaque ouverture de session.

Arrêt du mode service

© Copyright NETASQ 2006


Invite de commandes - UnInstallFwSyslog
C:\Program Files\Netasq\Administration Suite 5.0>UnInstallFwSyslog
C:\WINDOWS\system32\net.exe
The FW Syslog service has been shut down

Le service SYSLOG peut être désinstallé simplement en lançant « Retirer le Syslog » présent dans le menu :

« Démarrer>Programmes>Netasq>Administration Suite 5.0>Services »

Sinon, la procédure complète est la suivante :

1. Ouvrez une invite de commandes DOS,

2. Placez-vous dans le répertoire NETASQ de votre disque dur (en principe C:\Program Files\ netasq\Administration Suite x.x),

3. Tapez la commande de désinstallation du service : UnInstallFwSyslog.

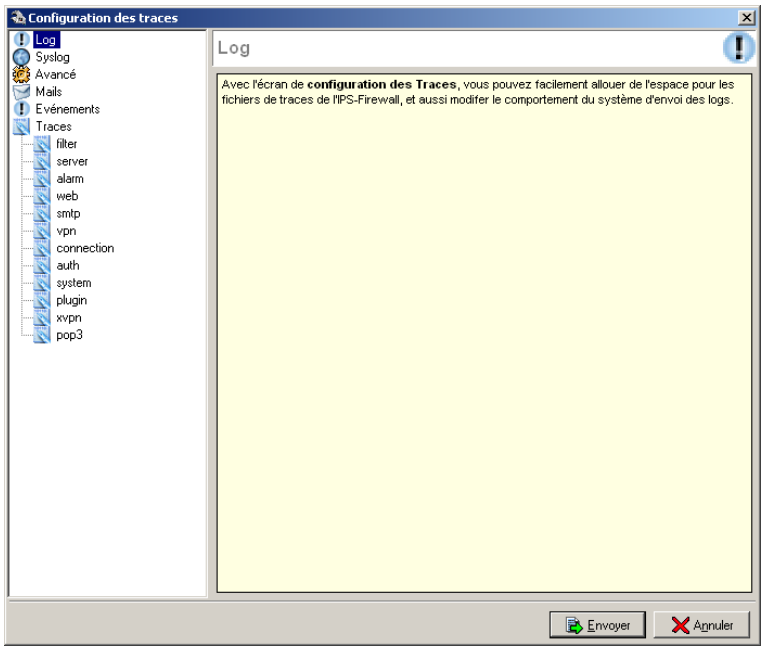
Attention : Il est important de redémarrer la machine afin de prendre en compte cette désinstallation.

Section B

Configuration

© Copyright NETASQ 2006

Pour utiliser le NETASQ SYSLOG, vous devez, au préalable, configurer un certain nombre de paramètres dans l'onglet Syslog du Menu « Traces ».



Etapes de la configuration

1. Activez l'option « Envoyer les messages au serveur syslog externe »,

2. Indiquez la machine d'administration sur laquelle est installé le NETASQ SYSLOG, laissez le port de connexion à la valeur 514,

3. Spécifier les types de traces qui seront envoyés du firewall au NETASQ SYSLOG (Alarme, Connexion, WEB, VPN, Authentification, Filtrage, SMTP, Système, Plugins…),

4. Le Log facility doit être sélectionné sur « aucun »,

5. Chiffrement du trafic : Le flux transitant entre le firewall et le NETASQ SYSLOG peut être chiffré en AES. Pour activer le chiffrement, sélectionnez l'option "Chiffrement du trafic" puis cliquez sur le bouton "Clé de chiffrement". Saisissez alors la clef de chiffrement utilisée (la même valeur de clef sera configurée sur le NETASQ SYSLOG). **Le chiffrement doit alors obligatoirement être activé sur le NETASQ SYSLOG.**

© Copyright NETASQ 2006

La configuration du NETASQ Syslog est réalisée par l'interface graphique installée avec les autres applications de la suite d'administration des produits NETASQ. Le NETASQ Syslog n'est pas installé par défaut, pour effectuer l'installation du NETASQ Syslog, il est nécessaire d'installer la suite d'administration dans les modes « Complète », « Serveur » ou « Personnalisée » de l'installation.

Une fois Installé l'interface graphique de configuration du NETASQ Syslog est disponible dans les menus des programmes, par défaut :

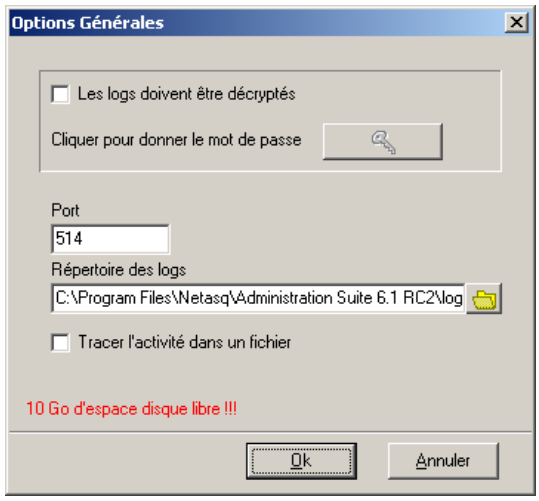
► Démarrer\Tous les programmes\Netasq\Administration Suite n°xx\Configure Syslog

Configuration du NETASQ SYSLOG

L'écran de configuration du NETASQ SYSLOG est constitué de deux menus :

► Fichiers : Démarrage, Arrêt et monitoring de l'activité du syslog ;
► Options : Options de la configuration du logiciel syslog, ce menu est constitué de trois menus « Général », « Tailles » et « Parsing ».

Général



Si vous avez activé le chiffrement des logs sur la console d'administration (Firewall Manager), vous devez obligatoirement activer l'option "Les traces doivent être décryptées" et saisir la clef de chiffrement utilisée (mot de passe).

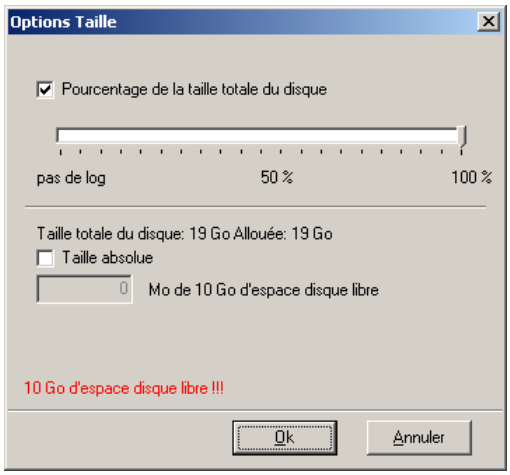
Dans le champ "Répertoire des logs", vous pouvez spécifier le chemin du répertoire de stockage des logs. Par défaut, les logs sont stockés dans le répertoire :

► C:\program files>Netasq>Administration Suite x.x>Log

Lorsque l'option « Tracer l'activité dans un fichier » est activée, toutes les opérations et les messages d'erreurs du NETASQ SYSLOG sont stockées dans un fichier. Ce fichier se trouve dans le répertoire des fichiers NETASQ (C:\program files>Netasq>Administration Suite x.x> par défaut) et se nomme SyslogtoFile.log.

© Copyright NETASQ 2006

Taille des traces



Cet onglet vous permet de déterminer la taille maximale allouée aux fichiers de traces sur le disque dur de la machine d'administration, ceci afin d'éviter la saturation de ce dernier.

Vous pouvez choisir une taille maximale relative ou absolue. La taille relative se calcule en pourcentage d'occupation du disque, la taille absolue se calcule en Moctets.

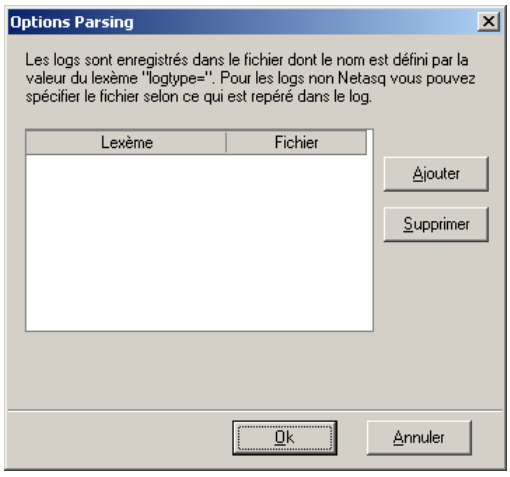
Taille relative

Pour définir une taille relative d'occupation, cochez la case "Pourcentage de la taille totale du disque" et choisissez la valeur désirée.

Taille absolue

Pour définir une taille absolue, cochez la case "Taille absolue" et saisissez la valeur absolue en Moctets.

Parsing


Options Parsing
Les logs sont enregistrés dans le fichier dont le nom est défini par la valeur du lexème "logtype=". Pour les logs non Netasq vous pouvez spécifier le fichier selon ce qui est repéré dans le log.
Lexème
Fichier
Ajouter
Supprimer
Ok
Annuler

Les traces sont enregistrées dans le fichier dont le nom est défini par la valeur du lexème « logtype= ». Pour les traces non NETASQ, il est possible de spécifier le fichier selon ce qui est repéré dans la ligne de traces. Ainsi ajoutez les mots clés de chaque ligne de traces pouvant être rencontrées en les associant à un fichier de traces NETASQ. Ainsi les traces non netasq récupérées par le syslog pourront être incluses dans les tableaux du reporter.

Si une ligne de trace ne correspond à aucun lexème configuré, elle ne peut être interprêtée par le syslog NETASQ et n'est donc pas prise en compte dans les tableau du reporter.

Section C

Exploitation des logs

© Copyright NETASQ 2006

L'analyse des logs récupérés par le NETASQ SYSLOG est réalisée au moyen du NETASQ REPORTER sans nécessiter de connexion à un firewall.

Reportez-vous à la notice du NETASQ REPORTER pour de plus amples renseignements sur l'exploitation des logs.

© Copyright NETASQ 2006

Emplacement des logs

Les logs sont stockés dans des fichiers texte, dans le répertoire choisi par l'administrateur. Par défaut, si l'administrateur n'a pas spécifié de répertoire particulier, le répertoire de log se trouve dans le chemin suivant :

C:\program files>Netasq>Administration Suite x.x>Log

Chaque jour, un nouveau fichier texte est créé pour chaque type de log (filtrage, connexion, alarme, SMTP, URL…). Le nom de chaque fichier est construit de la façon suivante :
<type de log>_<année>_<jour dans l'année>

Exemples

- alarm_2003_295.log
- connection_2003_291.log
- filter_2003_25.log
- web_2003_360.log
- smtp_2003_360.log

Chapitre XIII

Moniteur temps réel

© Copyright NETASQ 2006

Le moniteur temps réel vous permet de visualiser simplement l'activité de votre Firewall en temps réel. Il vous donne les informations suivantes :

- ► utilisation des ressources internes du Firewall (mémoire, CPU ...),
- ► liste des machines et utilisateurs connectés,
- ► alarmes remontées en temps réel,
- ► nombre de connexions, utilisation de la bande passante, débit,
- ► informations sur l'état des interfaces et des tunnels VPN
- ► derniers logs remontés,
- ► l'utilisation de l'espace disque alloué aux logs.

Vous pouvez, avec cet outil, vous connecter sur plusieurs firewalls et ainsi surveiller l'ensemble de votre parc de firewall.

Les menus

La fenêtre principale contient les menus suivants : « Firewall », « Applications », « Fenêtres » et « ? ».

Le menu **Firewall** vous permet de vous connecter aux firewalls et d'accéder aux options générales de l'application.

Le menu **Applications** vous permet de lancer directement les deux autres applications composant la suite d'administration NETASQ : le Firewall Manager et le Reporter.

Le menu **Fenêtres** vous permet d'organiser les fenêtres de connexion sur l'écran.

Le menu **?** vous permet d'accéder au présent fichier d'aide et de connaître la version du moniteur.

Le moniteur reçoit les informations du Firewall si il y est connecté. Vous pouvez ensuite le réduire avec le bouton de réduction de la fenêtre Windows . Le moniteur tourne alors en arrière plan. Pour le faire réapparaître à l'écran, double cliquez sur l'icône figurant au niveau de la barre des tâches (à côté de l'horloge à droite).

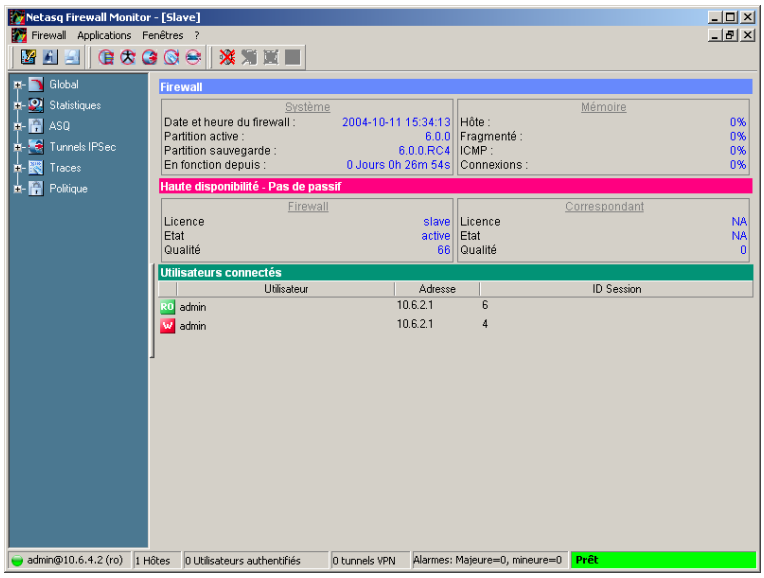
© Copyright NETASQ 2006

Section A

Fenêtre générale

© Copyright NETASQ 2006

Vous pouvez, à partir de cette fenêtre, ouvrir plusieurs fenêtres connectées chacune sur différents firewalls.



Firewall

Le menu Firewall concerne la connexion aux Firewalls et les options générales de l'application.

Connecter	Ouvre une nouvelle fenêtre de connexion à un Firewall. Entrez l'adresse IP du firewall et le mot de passe de l'utilisateur.
Carnet d'adresses	Configuration du carnet d'adresses de firewalls.
Préférences	Permet de régler la langue de l'interface, et quelques options de connexion.
Quitter	Déconnecte les moniteurs et quitte l'application.

Applications

Le menu Applications permet une connexion aux autres applications de la suite d'administration NETASQ. Utiliser les deux raccourcis procurent l'avantage de ne pas devoir se ré authentifier sur ces deux applications.

Lancer le Manager	Permet l'ouverture du Firewall Manager de la suite d'administration NETASQ.
Lancer le Reporter	Permet l'ouverture du Firewall Reporter de la suite d'administration NETASQ.

© Copyright NETASQ 2006

Fenêtres

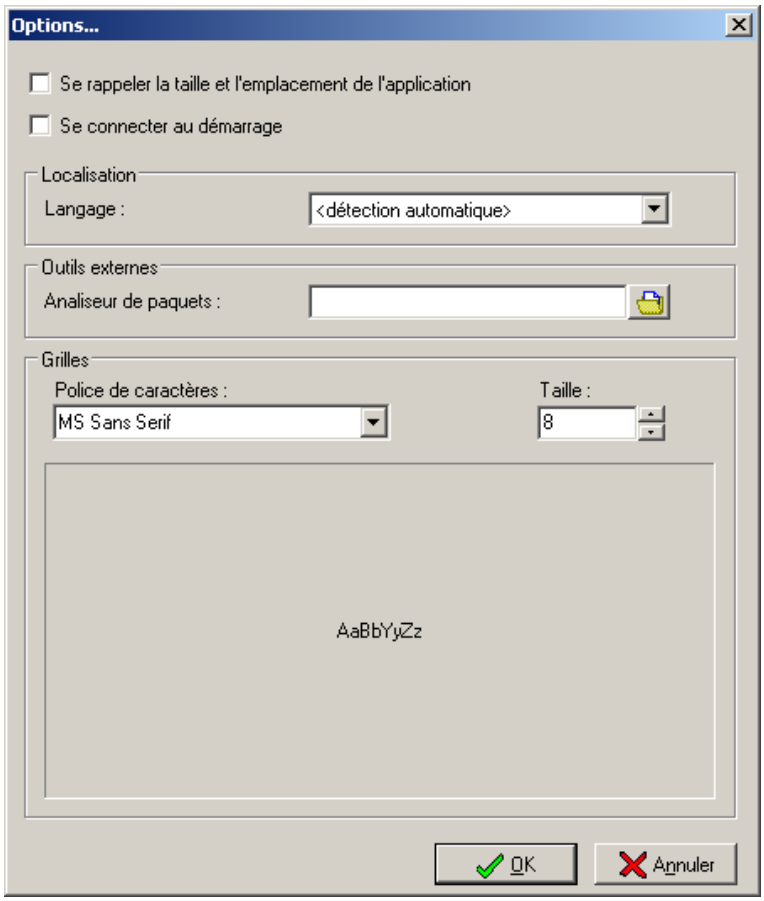
Le menu Fenêtres permet de gérer les fenêtres d'affichage des différents firewalls connectés :

Arranger les icônes	Aligne les fenêtres icônisées de connexion aux firewalls.
Cascade	Organise les différentes fenêtres connectées en cascade dans l'application.
Mosaïque	Organise les différentes fenêtres connectées en mosaïque dans l'application.
Charger une disposition	Charge un fichier contenant la disposition et taille des fenêtres sur l'écran.
Enregistrer la disposition	Sauvegarde la disposition et taille des fenêtres sur l'écran.
Liste des firewalls connectés	Permet de basculer vers une autre fenêtre active, repérée par l'adresse IP du firewall.

?

Aide	Ouvre l'Aide en ligne.
A propos ...	Donne des informations sur le moniteur utilisé (numéro de version, crédit).

Vous accédez à l'écran de configuration des préférences par le menu « Firewall > Préférences ».



Se rappeler la taille et la position de l'application

Option d'affichage, celle-ci permet de garder en mémoire la façon dont le monitor était disposé à l'écran (taille et position).

Se connecter au démarrage

Cette option permet de voir apparaître la fenêtre de connexion à chaque démarrage de l'application.

Langage de l'application

Vous pouvez choisir la langue des menus de l'interface. La sélection automatique prendra la langue de la version de Windows installée sur le poste. Après modification du choix, il faut redémarrer l'application pour activer le nouveau choix de langue.

Outils externes

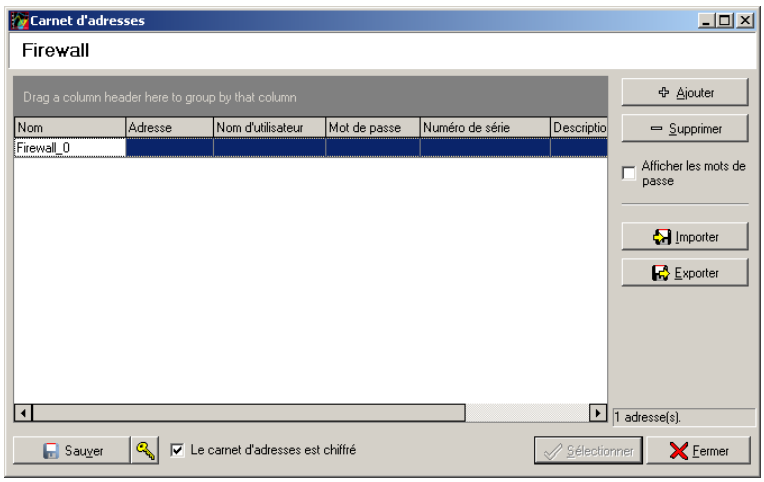
Lorsqu'une alarme se déclenche sur un IPS-Firewall NETASQ, il est possible de visualiser le paquet responsable du déclenchement de cette alarme. Pour cela il faut vous munir d'un outil de visualisation de paquets comme Ethereal ou Packetyzer… Spécifiez l'outil choisi dans le champ « Analyseur de paquets», celui ci sera utilisé par le monitor pour afficher les paquets malicieux.

Grille

Enfin, il vous est possible de définir une police et sa taille pour l'affichage des logs dans la grille.

© Copyright NETASQ 2006

Vous accédez au carnet d'adresses par le menu « Firewall > Carnet d'adresses » ou en appuyant sur l'icône situé à côté du champ adresse dans le popup de connexion.



Vous avez la possibilité de mémoriser les informations de connexion sur vos différents firewalls. Ces informations sont stockées sur le poste client où est installée l'interface. Elles peuvent être chiffrées si vous cochez l'option « Chiffrement du carnet d'adresses ». Dans ce cas, une clé de chiffrement vous est demandée. Les informations mémorisées sont l'adresse IP, le login, le mot de passe de connexion et le numéro de série de l'IPS-Firewall auquel vous souhaitez vous connectez. Le mot de passe est celui d'un utilisateur autorisé.

En spécifiant un numéro de série vous vous prévenez contre les attaques de type « man in the middle ». En effet si vous tentez une connexion sur un équipement qui ne répond pas au critère « Numéro de série » indiqué dans le carnet d'adresses, le monitor vous indique que vous êtes en train de tenter une connexion sur un équipement inconnu. Il vous demande si vous désirez rajouter ce numéro dans la liste autorisée. Vérifiez bien les informations affichées par le monitor avant d'accepter une telle requête.

Une fois les informations entrées, vous pouvez les sauvegarder avec le bouton "Enregistrer". Pour ouvrir une session sur un des firewalls du carnet d'adresses, cliquez sur le nom de ce dernier puis sur le bouton "sélectionner" ou double cliquez sur ce même nom.

Attention, si vous modifiez l'option « Chiffrement du carnet d'adresses », il faut enregistrer à nouveau le carnet pour prendre en compte les modifications.

Cochez l'option « Voir les mots de passe » pour vérifier les mots de passe utilisés pour chacun des IPS-Firewalls enregistrés dans le carnet d'adresses (les mots de passe sont affichés en clair).

© Copyright NETASQ 2006

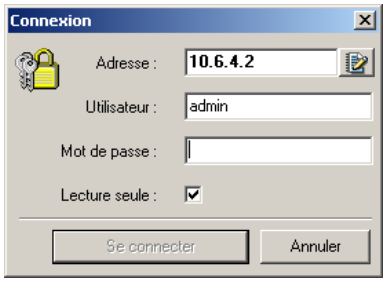
Section B

Fenêtre du moniteur

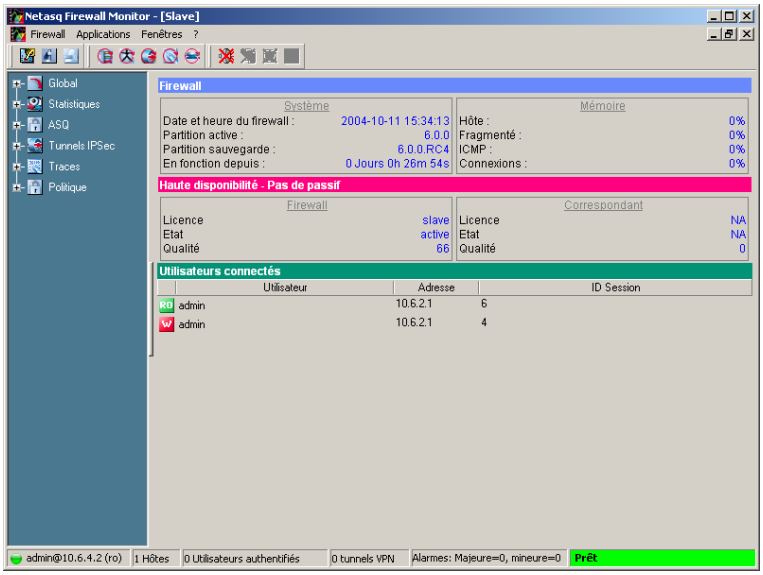
© Copyright NETASQ 2006

L'ouverture d'un moniteur se fait par le biais du menu « Firewall > Connecter » de l'application.

Une fenêtre d'ouverture de session apparaît.



Vous pouvez alors indiquer l'adresse IP du firewall auquel se connecter et le mot de passe de l'utilisateur. Vous avez la possibilité de mémoriser les adresses IP et mots de passe dans un carnet d'adresses chiffré, accessible avec l'icône . (cf rubrique carnet d'adresses). Une fois connecté, la fenêtre principale du moniteur apparaît.



© Copyright NETASQ 2006

La fenêtre du moniteur vous apporte un certain nombre d'informations sur l'activité du firewall.

Elle est décomposée en quatre parties :

► une barre horizontale contenant de petites icônes et permettant le rafraîchissement des informations contenues dans la zone d'affichage,

► une barre verticale contenant l'arborescence des menus et permettant la visualisation et le paramétrage des options du Firewall Monitor,

► une zone d'affichage des résultats,

► une barre d'état.

Descriptif des petites icônes

	Accéder au menu d'options de cette fenêtre.
	Connexion
	En cliquant sur ce bouton, vous générez un rapport au format HTML. Ce rapport contient les informations suivantes, à un instant t : ► liste des machines connectées (adresse IP, interface à laquelle est rattaché l'utilisateur, quantité de données transférées, nombre de connexions, débit utilisé ...), ► liste des utilisateurs authentifiés (nom de l'utilisateur, IP, temps d'authentification restant...), ► liste des alarmes remontées, ► liste des tunnels VPN actifs.
	Rafraîchir la liste des machines connectées.
	Rafraîchir la liste des utilisateurs authentifiés.
	Rafraîchir la liste des tunnels VPN.
	Rafraîchir la liste des logs.
	Rafraîchir la liste des informations de HA.
	Effacer les alarmes affichées dans le Firewall Monitor.
	Effacer les statistiques.
	Déconnecter les utilisateurs authentifiés.
	Vider la quarantaine, toutes les machines et utilisateurs en quarantainre sont donc libérés.

© Copyright NETASQ 2006

	Démarrer Active Update permet un démarrage manuel de la fonctonnalité Active Update des IPS-Firewalls.

Arborescence des menus

Cette barre est composée de six sections :

► **Global :** cette section concentre les informations générales sur les traces et les services du firewall,

► **Statistiques :** cette section vous permet de visualiser des graphiques temps réel concernant la bande passante, le débit et les connexions,

► **ASQ :** dans cette zone vous pouvez contrôler des tableaux temps réel concernant les hôtes, les utilisateurs authentifiés et les alarmes remontées par le firewall,

► **VPN :** ce menu vous présente les tunnels VPN en cours,

► **Logs :** affichage des derniers logs sur « xx » lignes (xx, cette information est paramétrable, grâce à l'icône « options » décrit ci-dessus).

► **Politique** : visualisation des slots (filtrage, filtrage d'URL, VPN, Filtrage global, NAT) et affichage de la politique de filtrage complète actuellement active (règles implicites, règles de filtrage global, règles de filtrage local).

Les configurations relatives à ces menus sont décrites dans la suite du manuel.

Zone d'affichage des résultats

Dans cette zone apparaissent les données et options des menus sélectionnés dans la barre horizontale. Le détail de ces écrans est traité dans les sections correspondantes.

Barre d'état

Cette barre est constituée de 6 zones d'information :

► une zone de texte affichant l'utilisateur connecté sur quel firewall sous la forme : <utilisateur_connecté>@<adresse_IP_firewall>,

► une zone affichant le nombre d'hôtes ayant établi une connexion avec le firewall,

► une zone affichant le nombre d'utilisateurs authentifiés,

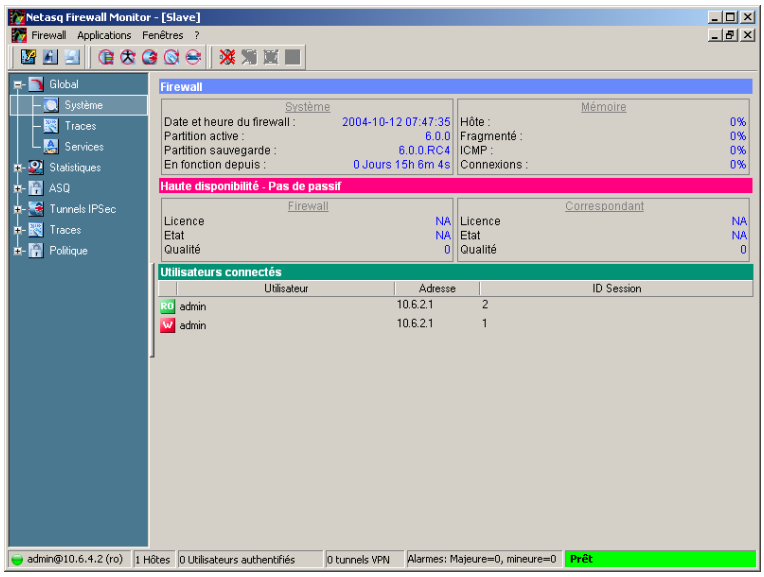
► une zone affichant le nombre de tunnels VPN,

► une zone affichant le nombre d'alarmes remontées par le firewall,

► une zone affichant l'état de l'application (un traitement est en cours ou non, respectivement bleu ou vert).

© Copyright NETASQ 2006

Information Système



Système

Partition active et partition sauvegarde	Version des différentes partitions du firewall.
En fonction depuis	Jours, heures, minutes et secondes depuis le dernier démarrage du firewall.

Mémoire

C'est le pourcentage d'utilisation d'une mémoire (buffer) réservée au stockage d'informations. Ce stockage d'informations est lié au stateful et correspond à l'enregistrement du contexte.

Hôtes	Pile des hôtes.
Fragmenté	Paquets découpés.
ICMP	Requêtes ICMP (ping, traceroute...).
Connexions	L'ensemble des connexions TCP/IP.

Les dimensions des buffers varient en fonction des types de produits (F50, F10, F100, F500, F100C, ...) et des versions de produit (3.36, 3.41, 3.5, 4.0...).

Des algorithmes de nettoyage optimisent le fonctionnement des buffers des "Hôtes", "Fragmenté", "ICMP" et "Connexions". Les entrées dans les buffers "Fragmenté" et "ICMP" sont initialisées à intervalles fixes (chaque entrée a une durée de vie limitée : TTL).

Cela illustre une partie de la charge du boîtier firewall. Un pourcentage trop élevé correspond à une surcharge du firewall ou à une attaque.

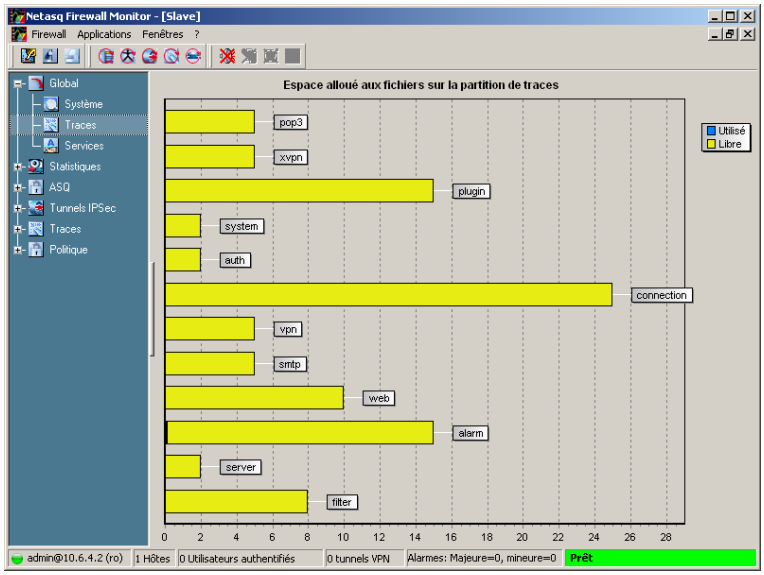
Si la haute disponibilité est activée, une section supplémentaire vous donne les informations relatives à la haute disponibilité (Etat des firewalls, des licences, synchronisation).

© Copyright NETASQ 2006

Utilisateurs connectés

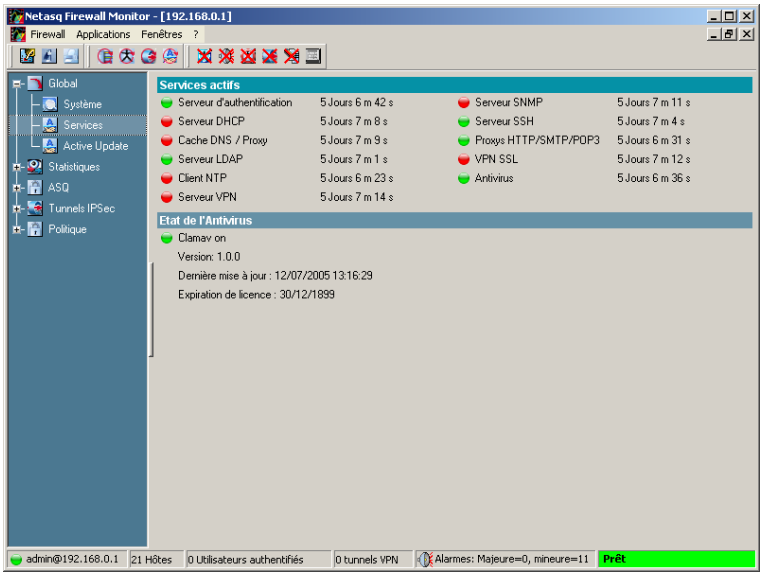
La section « Utilisateurs connectés » permet la visualisation des différents utilisateurs actuellement connectés sur l'IPS-Firewall, dans le cadre d'une session d'administration. La grille présente quatre informations : le login de l'utilisateur, ses droits (RO pour « Read Only » droits de lecture uniquement, W pour « Write » privilèges de modification, M pour « Mon_Write » droits de modification sur le Monteur uniquement), l'adresse IP depuis laquelle l'utilisateur est connecté et enfin un identifiant de connexion.

Traces



Un graphique représente en temps réel la taille actuelle du fichier de logs (filter, server, alarm, WEB, SMTP, VPN, connection, auth, system, plugin, xvpn, pop3) par rapport à la taille allouée sur le firewall pour chaque type de traces.

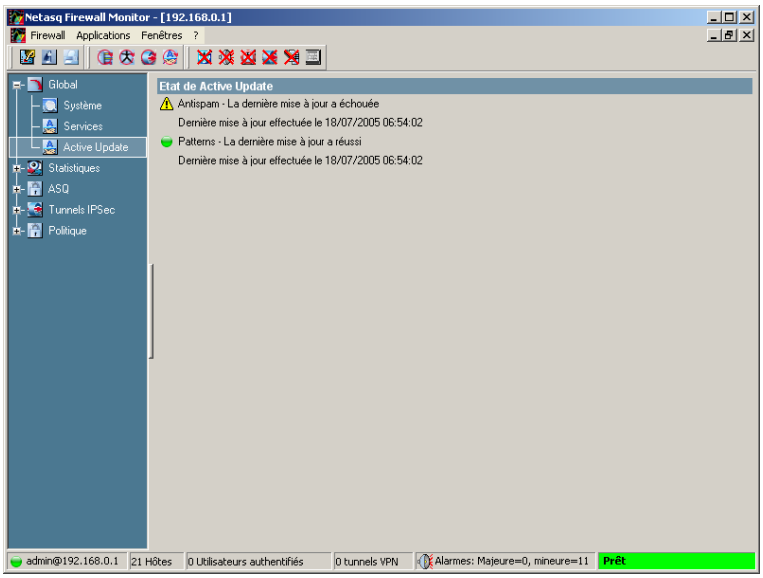
Services actifs


Netasq Firewall Monitor - [192.168.0.1]
Firewall Applications Fenêtres ?
Global
Système
Services
Active Update
Statistiques
ASQ
Tunnels IPSec
Politique
Services actifs
Serveur d'authentification 5 Jours 6 m 42 s
Serveur DHCP 5 Jours 7 m 8 s
Cache DNS / Proxy 5 Jours 7 m 9 s
Serveur LDAP 5 Jours 7 m 1 s
Client NTP 5 Jours 6 m 23 s
Serveur VPN 5 Jours 7 m 14 s
Serveur SNMP 5 Jours 7 m 11 s
Serveur SSH 5 Jours 7 m 4 s
Proxys HTTP/SMTP/POP3 5 Jours 6 m 31 s
VPN SSL 5 Jours 7 m 12 s
Antivirus 5 Jours 6 m 36 s
Etat de l'Antivirus
Clamav on
Version: 1.0.0
Dernière mise à jour : 12/07/2005 13:16:29
Expiration de licence : 30/12/1899
admin@192.168.0.1
21 Hôtes
0 Utilisateurs authentifiés
0 tunnels VPN
Alarmes: Majeure=0, mineure=11
Prêt

Cette fenêtre énumère les services (actifs et non actifs) présents sur le firewall et depuis combien de temps ils ont été activés/désactivés.

Cette fenêtre contient aussi des informations concernant l'antivirus (activité, version, dernière mise à jour, l'expiration de la licence).

Active Update



Enfin la dernière section de la fenêtre affiche l'état de l'Active Update sur l'IPS-Firewall pour chaque type de mise à jour disponible (Antispam, Antivirus, Signatures Contextuelles, URL dynamiques) L'écran du moniteur précise le résultat de la dernière mise à jour effectuée (échouée ou réussie) et la date de la dernière mise à jour.

Présentation

Les statistiques sont affichées sous forme de graphiques. Ceux-ci sont présentés en 3 dimensions.

Les deux axes verticaux et horizontaux sont gradués.

La graduation horizontale est horaire. La graduation verticale est soit :

- un pourcentage de bande passante,
- un débit en octet, kilo octet ou mega octet,
- un nombre de connexions.

Le troisième axe transversal est illustré par des bandes de couleurs différentes. Une légende à droite du graphique donne la correspondance entre la couleur et le type, le fait qu'elle soit active ou non et le nom de l'interface.

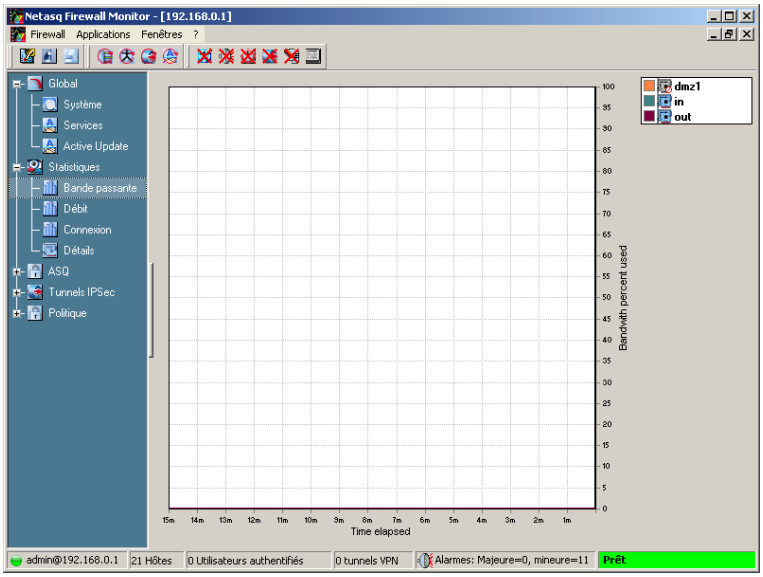
En cliquant sur une interface dans la légende, vous pouvez masquer ou afficher le graphique correspondant à cette interface (le graphique est masqué lorsque le nom de l'interface est grisé dans la légende). La couleur attribuée à l'interface est celle définie dans le Firewall Manager.

Le type des interfaces

- Interface réseau classique active,
- Interface de type VLAN active,
- Interface de type Dialup active,
- Interface de type PPTP active,
- Interface classique désactivée.

Les trois autres types d'interface (VLAN, PPTP ou DIALUP) lorsqu'elles sont désactivées apparaissent en gris ou n'apparaissent pas.

Bande passante



© Copyright NETASQ 2006

Le diagramme Bande passante affiche en temps réel le pourcentage d'utilisation de la bande passante disponible sur chaque interface.

Chaque interface est représentée par une couleur différente dont la légende figure à droite du diagramme.

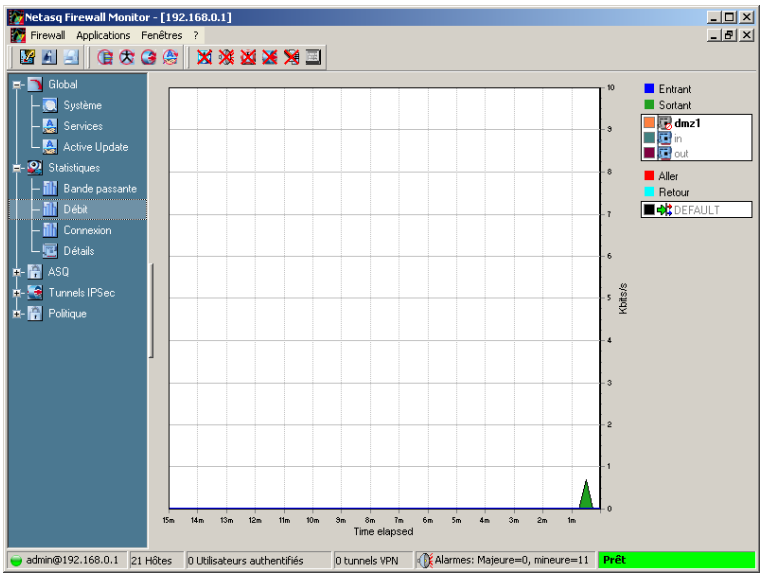
Le maximum de bande passante représente le débit théorique maximum supporté par l'interface.

Par exemple, pour une ligne à 100 Mbit/s utilisée en full duplex, ce maximum sera de 200 Mbit/s alors que pour une ligne à 10 Mbit/s en half duplex, ce maximum sera de 10 Mbit/s.

Un double clic sur le diagramme vous permet de diviser cette période de visualisation en deux et ceci deux fois avant de revenir à l'échelle d'origine.

Cliquez sur une interface dans la légende en haut à droite du graphique désactive la visualisation de cette interface dans le graphique.

Débit



Le diagramme de débit représente le débit réel sur chaque interface du Firewall au cours de la période définie. Cette période est paramétrable dans les options de la fenêtre. L'échelle des débits s'adapte automatiquement au débit maximal enregistré au cours de la période.

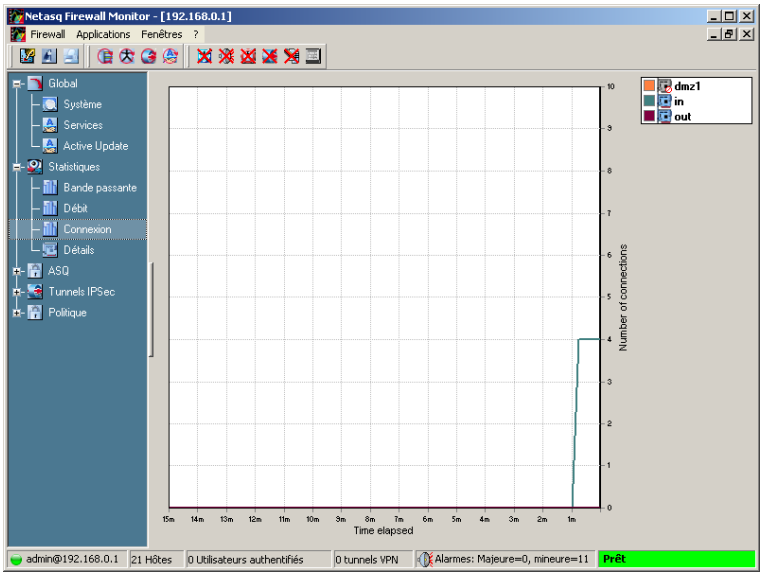
Un double clic sur le diagramme vous permet de diviser cette période de visualisation en deux et ceci deux fois avant de revenir à l'échelle d'origine.

Pour chaque interface le graphique de débit indique le débit sortant et le débit entrant. Il est aussi possible de visualiser dans cette section les différents débits (sens de la définition de la règle et sens inverse) des files d'attente de la QoS. Par défaut, lorsqu'il n'y a pas de règle de QoS configurée, c'est la règle de QoS « Default » qui est affichée.

Pour modifier l'interface sur laquelle sont visualisées les débits, cliquez sur cette interface dans la légende en haut à droite du graphique. L'interface en cours de visualisation est indiquée en gras.

© Copyright NETASQ 2006

Connexion



Le diagramme de connexion affiche en temps réel le nombre de connexions sur chaque interface du Firewall au cours de la période définie.

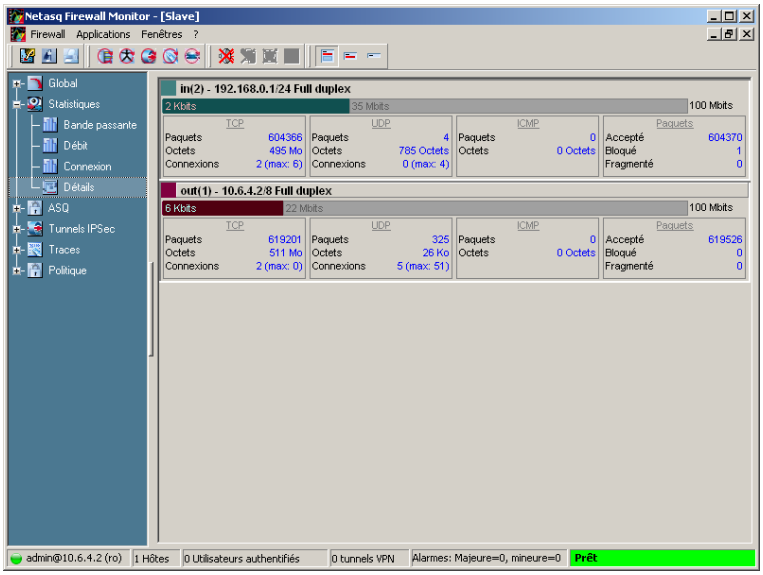
Chaque interface est représentée par une couleur différente dont la légende figure à droite du diagramme.

La période est paramétrable dans les options .

Un double clic sur le diagramme vous permet de diviser cette période de visualisation en deux et ceci deux fois avant de revenir à l'échelle d'origine.

Cliquez sur une interface dans la légende en haut à droite du graphique désactive la visualisation de cette interface dans le graphique.

Détails



© Copyright NETASQ 2006

Chaque tableau synthétise des informations statistiques de débit pour chacune des interfaces :

► le nom, l'adresse IP, le masque de sous réseau en formulation américaine (voir explications en annexe) , le type de connexion (10 ou 100Mbit, half duplex ou full duplex),
► le débit instantané (à gauche) et maximum (à droite),
► le nombre de paquets et le volume en octets pour les protocoles TCP, UDP, ICMP,
► le nombre de connexions TCP,
► le nombre total de paquets acceptés, bloqués et fragmentés par le firewall.

Les interfaces déconnectées apparaissent grisées.

D'autre part, il est possible, par un clic de souris sur le nom de l'interface ou la flèche colorée, de déployer ou limiter les informations visibles au :

► nom seul,
► au nom et débit total,
► au nom, débit total et détaillé.

Les trois boutons suivants vous permettent respectivement :

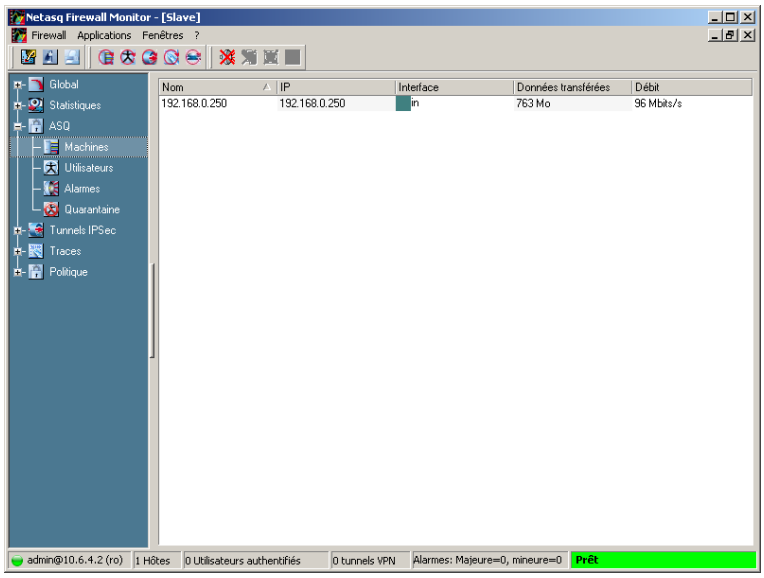
► d'afficher toutes les informations pour toutes les interfaces,
► d'afficher uniquement la barre de débits pour toutes les interfaces,
► de n'afficher aucune information.

Vous remarquerez aussi les couleurs des interfaces visibles sur la droite de la fenêtre. Il s'agit de la couleur définie dans les paramètres réseau du Firewall Manager pour chacune des interfaces (reportez vous au chapitre II « définition des interfaces »).

Le menu ASQ présente les informations remontées par l'ASQ et capturée par le moniteur. Affichées sous forme de tableaux, ces informations concernent :

- ► Les machines,
- ► Les uitlisateurs,
- ► Les alarmes,
- ► La quarantaine.

Machines



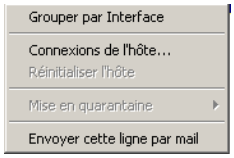
En cliquant sur l'onglet Machines, vous affichez les données suivantes :

Nom	Nom de la machine émettrice (si déclarée dans les objets) ou adresse IP de la machine (dans le cas contraire).
IP	Adresse IP de la machine émettrice.
Interface	Interface à laquelle est connecté l'hôte.
Données sortantes	Nombre d'octets ayant transités par le Firewall à destination de la machine émettrice depuis le démarrage du Firewall.
Données entrantes	Nombre d'octets ayant transités par le Firewall à partir de la machine émettrice depuis le démarrage du Firewall.
Débit sortant	Débit réel des flux à destination de la machine et transitant par l'IPS-Firewall.
Débit entrant	Débit réel des flux provenant de la machine et transitant par IIPS-Firewall.

Remarque

Vous pouvez trier la grille en cliquant sur la colonne que vous désirez classer.

Menu contextuel



En cliquant sur le bouton droit de la souris, vous avez accès à un menu contextuel qui vous donne les possibilités suivantes :

► Grouper par interface : vous pouvez grouper les hôtes connectés par interface pour une meilleure visibilité de la topologie réseau,

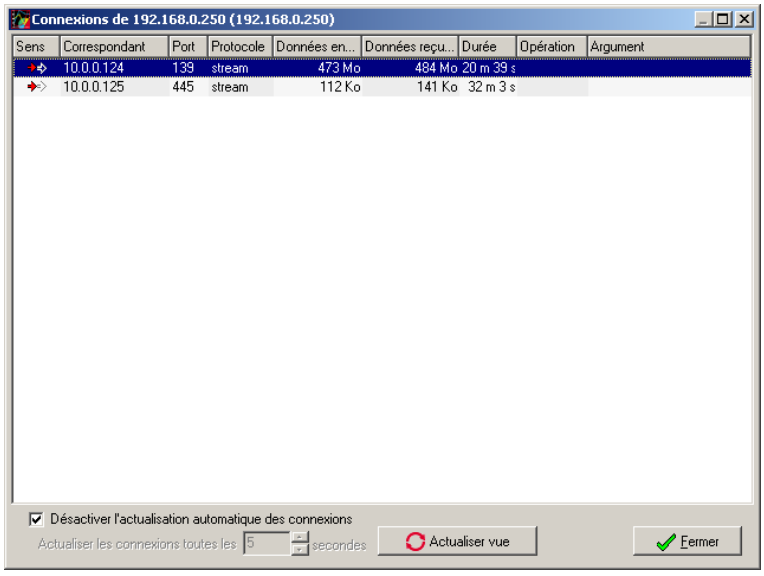
► Connexions pour cet hôte : cet écran vous permet de visualiser les différentes connexions en cours pour l'hôte concerné,

► Réinitialiser l'hôte : remise à zéro instantanée des statistiques de l'hôte en question.

► Mise en quarantaine : blocage dynamique de la machine mise en quarantaine pour une durée à spécifier.

► Envoyer cette ligne par mail : ouverture du client de messagerie avec la ligne sélectionnée, indiquée dans le corps du message.

Connexions pour l'hôte sélectionné



En cliquant sur l'option « Connexions pour cet hôte », vous affichez les données suivantes :

Sens	Sens du trafic : ( ) : représente une connexion sortante par rapport au firewall, ( ) : représente une connexion entrant par rapport au firewall.
Correspondant	Interface à laquelle est connecté l'hôte.
Port	numéro de port.
Protocole	protocole de la connexion.
Données envoyées	quantité de données envoyées.
Données reçues	quantité de données reçues.
Durée	temps de la connexion.

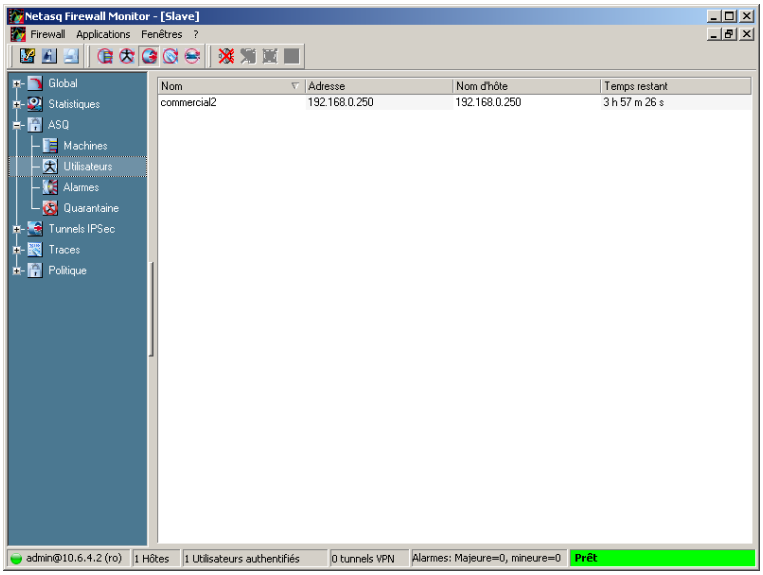
© Copyright NETASQ 2006

Opération	commande identifiée du protocole.
Argument	paramètre de l'opération.

En décochant l'option « Désactiver l'actualisation automatique des connexions » vous désactivez le rafraîchissement automatique des informations de connexions de la fenêtre. Ce rafraîchissement est effectué selon le temps indiqué par le paramètre « Actualiser les connexions toutes les ».

Vous avez toujours la possibilité de rafraîchir manuellement les informations de connexions visualisées en cliquant sur le bouton « Actualiser vue ».

Utilisateurs



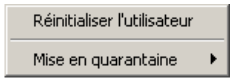
En cliquant sur l'onglet Utilisateurs, vous affichez les données suivantes :

Nom	Nom de l'utilisateur authentifié.
Adresse	Adresse IP de l'utilisateur.
Nom d'hôte	Nom de l'hôte s'il a été renseigné dans les objets.
Temps restant	Temps restant pour l'authentification. (Un utilisateur est authentifié pour une certaine durée).

Remarque

Vous pouvez trier la grille en cliquant sur la colonne que vous désirez classer. L'icône apparaîtra en rouge si l'utilisateur s'est authentifié depuis l'extérieur.

Menu contextuel

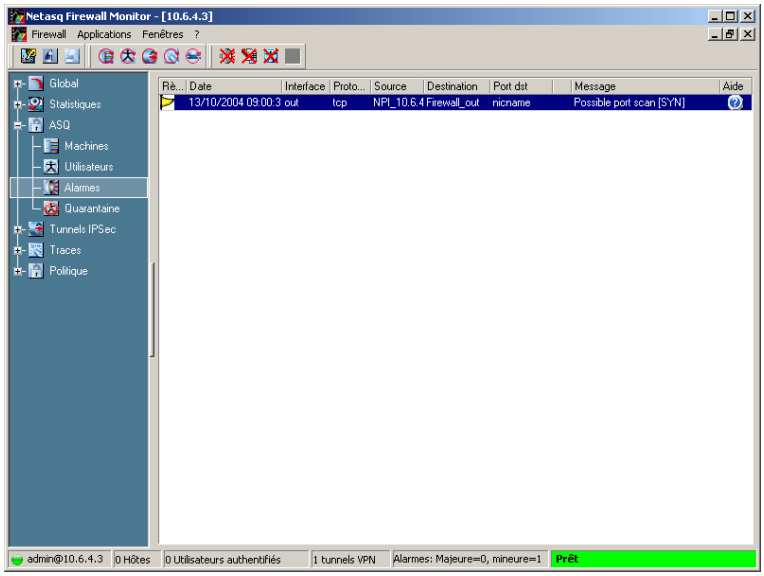


En cliquant sur le bouton droit de la souris, vous avez accès à un menu contextuel qui vous donne les possibilités suivantes :

► Purger cet utilisateur : déconnexion instantanée de l'utilisateur authentifié en question.

© Copyright NETASQ 2006

Alarmes



Les alarmes déclenchées par le Firewall apparaîtront dans cette fenêtre.

En cliquant sur l'onglet alarmes, vous affichez les données suivantes :

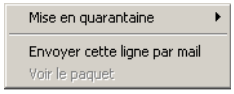
Règle	Criticité de l'alarme.
Date	Date et heure de déclenchement de l'alarme.
Interface	Nom de l'interface du Firewall sur laquelle s'est déclenchée l'alarme.
Protocole	Protocole du paquet qui a déclenché l'alarme.
Source	Adresse IP de la machine source du paquet qui a déclenché l'alarme.
Destination	Adresse IP de la machine destinataire du paquet qui a déclenché l'alarme.
Port dst	Port demandé pour cette connexion.
Dump	Cette colonne indique par un petit icône que le paquet qui a provoqué la remontée de l'alarme a été sauvegardé. Cliquez sur ce bouton pour afficher le paquet (nécessite qu'un analyseur de paquet soit configuré). Voir « Préférences ».
Message	Informations complémentaires sur l'alarme.
Aide	Accès à une aide complémentaire sur l'alarme.

On distingue les alarmes majeures et mineures par le petit drapeau en début de ligne, rouge pour les premières et jaune pour les autres.

Remarque

Vous pouvez trier la grille en cliquant sur la colonne que vous désirez classer.

Menu contextuel



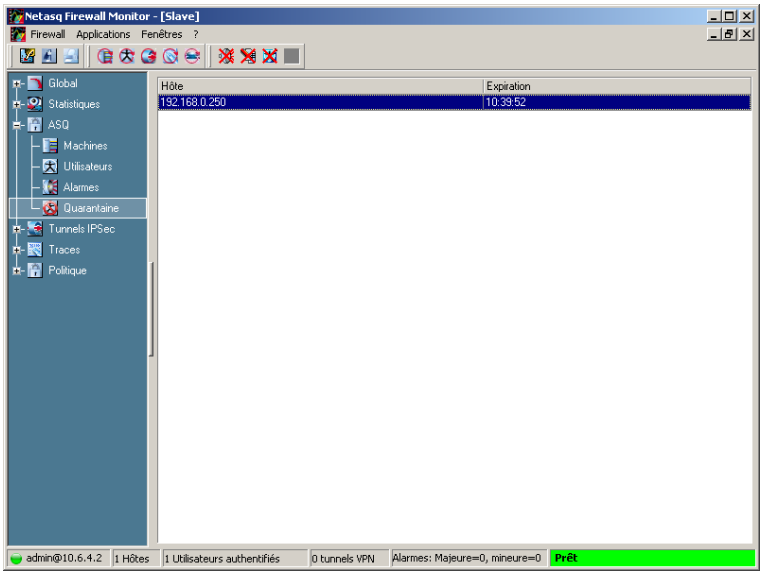
En cliquant sur le bouton droit de la souris, vous avez accès à un menu contextuel qui vous donne les possibilités suivantes :

► Mise en quarantaine : blocage dynamique de la machine mise en quarantaine pou une durée à spécifier.

► Envoyer cette ligne par mail : ouverture du client de messagerie avec la ligne sélectionnée, indiquée dans le corps du message.

► Voir le paquet : permet d'afficher le paquet (nécessite qu'un analyseur de paquet soit configuré) Voir « Préférences ».

Quarantaine



Cette fenêtre présente les machines qui ont été placées en quarantaine dynamique. Les machines en quarantaine statique (Voir « Configuration de la quarantaine statique ») ne sont pas représentées dans cette liste. En cliquant sur l'onglet « Quarantaine », vous affichez les données suivantes :

Hôte	Indique l'hôte actuellement en quarantaine.
Expiration	Heure d'expiration de la quarantaine.

Menu contextuel

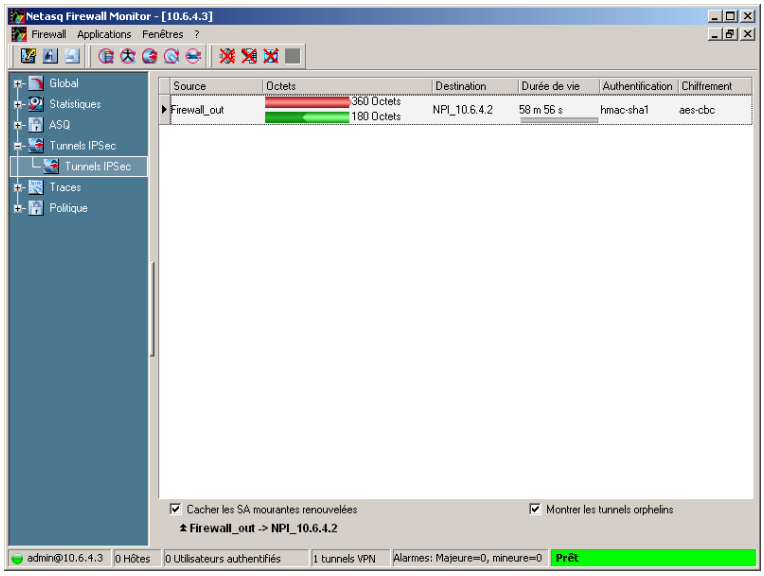
En cliquant sur le bouton droit de la souris, vous avez accès à un menu contextuel qui vous donne les possibilités suivantes :

► Retirer : pour retirer l'hôte sélectionné de la liste de quarantaine,

► Vider la quarantaine : retire toutes les machines de la quarantaine.

Tunnels IPSEC

En cliquant sur l'onglet VPN, vous affichez les données suivantes.



On trouve, dans une première partie, des informations statistiques sur le fonctionnement du tunnel :

► l'IP de l'initiateur du tunnel,
► les débits,
► l'IP de destination,
► la durée de vie de la SA (Security Association) par une représentation graphique de la position dans cette durée de vie ainsi que la valeur chiffrée (heures, minutes, secondes),
► le nom de l'algorithme d'authentification,
► le nom de l'algorithme de chiffrement.
► Des messages d'erreurs dans l'établissement du tunnel.

Le tunnel se décompose en deux sous-tunnels, un dans un sens, un dans l'autre sens de circulation des datagrammes.

On trouve, dans une deuxième partie (accessible en cliquant sur l'intitulé du tunnel situé en bas de page), des informations de type SAD (Security Association Database) :

► les adresses IP source et destination,
► le mode tunnel ou transport,
► le numéro de "SPI" (Security Parameter Index) entrant et le numéro de SPI sortant qui sont les identifiants de la SA (Security Association),
► le "Reqid" : numéro de séquence, indicateur utilisé pour le service d'anti-rejeu,
► l'algorithme d'authentification,
► l'algorithme de chiffrage,
► l'état de la SA.

Cet état est représenté par un code couleur. La ligne contenant les informations du VPN prendra une des couleurs suivantes en fonction de l'état du tunnel.

	état non déterminé.

© Copyright NETASQ 2006

	Larval : la SA est en cours de négociation ou n'a pas été complètement négociée.
	Mature : la SA est établie et disponible, le tunnel VPN est correctement monté.
	Dying : la SA va bientôt expirer, une nouvelle SA est en cours de négociation.
	Dead : la SA est expirée et inutilisable, le tunnel n'a pas été remonté et n'est donc plus actif.
	Orphan : un problème a été rencontré, généralement cet état signifie que le tunnel n'est monté que dans un seul sens.

► le protocole de sécurité : ESP ou AH,
► le nombre d'octets et la limitation maximum en octets (0 signifie : pas de limite maximum),
► le temps de vie de la SA et la durée de vie maximum en secondes (0 signifie : pas de limite maximum) (ici le chiffre est de 600, ce qui correspond à 10 min).

Les algorithmes et les limites maximum ont été configurés dans le Firewall Manager (référez-vous à l'aide de Firewall Manager pour plus de détail).

Vous trouverez d'autres informations sur les paramètres visibles dans cette fenêtre en vous référant à la RFC.

Des informations complémentaires peuvent être trouvées dans la RFC 2401 IPSEC :
http://www.ietf.org/rfc/rfc2401.txt
ou sur d'autres sites tel que : http://www.guill.net/reseaux/Ipsec.html

Deux options sont disponibles dans ce menu :

Cacher les SA mourantes renouvelées.	Permet de cacher les SA expirées qui ont été renouvelées.
Montre les tunnels orphelins	Permet d'afficher les tunnels qui sont actuellement dans l'état « Orphelin » ou « Orphan ». Les différents états sont indiqués ci-dessus.

Menu contextuel

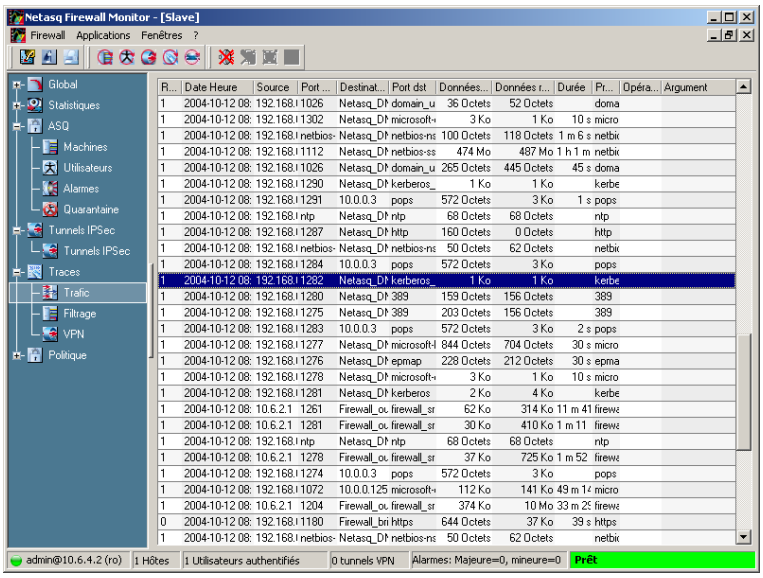
En cliquant sur le bouton droit de la souris, vous avez accès à un menu contextuel qui vous donne les possibilités suivantes :

► Fermer le tunnel : le tunnel sélectionné est supprimé, la configuration sur les IPS-Firewalls est toujours active,

► Tout réinitialiser : tous les tunnels sont supprimés.

Le Firewall monitor de la suite d'administration de NETASQ est un outil de monitoring temps réel des firewalls NETASQ. Il ne permet donc pas de faire un suivi (au long terme) de l'activité tracée (logs). Toutefois vous avez la possibilité de visualiser un certain nombre des logs les plus récents. Vous pouvez configurer le nombre de lignes de logs que vous voulez visualiser dans les options du monitor (Chapitre XII –Section C « Options »).

Trafic

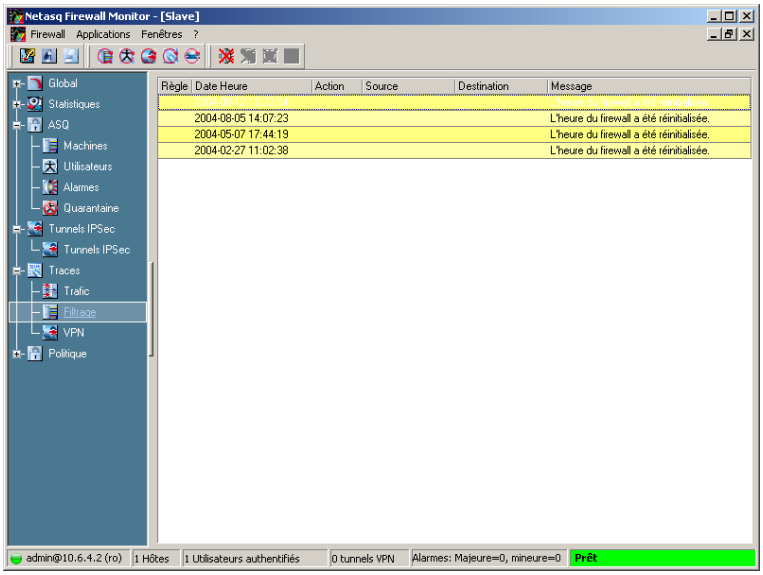


En cliquant sur l'onglet Trafic, vous affichez les données suivantes :

Règle	Identifiant de la règle.
Date Heure	Date et heure de génération de la ligne de logs.
Source	Adresse IP ou nom résolu de la source.
Port src	Numéro de port de la source.
Destination	Adresse IP ou nom résolu de la destination.
Port dst	Numéro de port de la destination.
Données envoyées	Quantité de données envoyées.
Données reçues	Quantité de données reçues.
Durée	Temps de la connexion.
Protocole	Protocole de la connexion.
Opération	Commande identifiée du protocole.
Argument	Paramètre de l'opération.

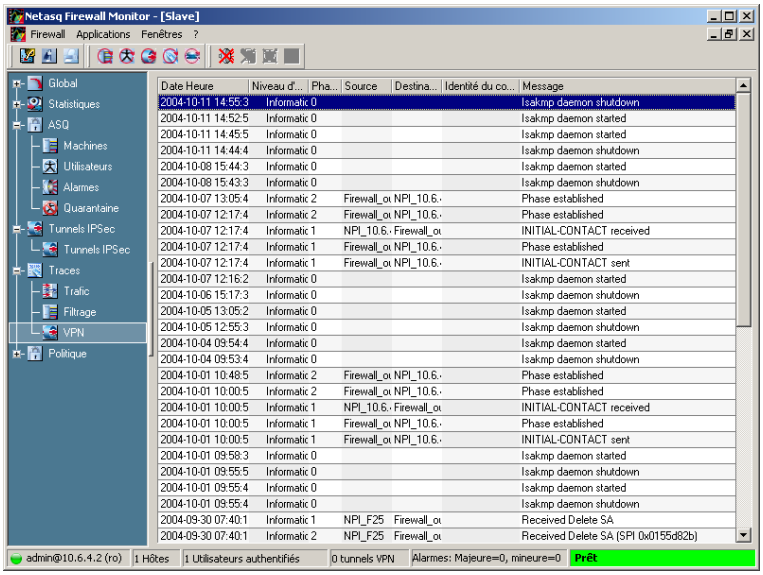
© Copyright NETASQ 2006

Filtrage



En cliquant sur l'onglet Filtrage, vous affichez les données suivantes :

Règle	Identifiant de la règle.
Date Heure	Date et heure de génération de la ligne de logs.
Niveau	Pour les alarmes, niveau de l'alarme (majeur ou mineur).
Action	Action de la règle de filtrage : « none », « pass », « block », « reset » respectivement aucune (règle qui n'a pas d'effet), passer, bloquer.
Source	Adresse IP de la source.
Destination	Adresse IP de la destination.
Message	Alarme.


Netasq Firewall Monitor - [Slave]
Firewall Applications Fenêtres ?
Global
Statistiques
ASQ
Machines
Utilisateurs
Alarmes
Quarantaine
Tunnels IPSec
Tunnels IPSec
Traces
Trafic
Filtrage
VPN
Politique
Date Heure Niveau d'... Pha... Source Destina... Identité du co... Message
2004-10-11 14:55:3 Informatic 0 Isakmp daemon shutdown
2004-10-11 14:52:5 Informatic 0 Isakmp daemon started
2004-10-11 14:45:5 Informatic 0 Isakmp daemon started
2004-10-11 14:44:4 Informatic 0 Isakmp daemon shutdown
2004-10-08 15:44:3 Informatic 0 Isakmp daemon started
2004-10-08 15:43:3 Informatic 0 Isakmp daemon shutdown
2004-10-07 13:05:4 Informatic 2 Firewall_ot NPI_10.6. Phase established
2004-10-07 12:17:4 Informatic 2 Firewall_ot NPI_10.6. Phase established
2004-10-07 12:17:4 Informatic 1 NPI_10.6. Firewall_ot INITIAL-CONTACT received
2004-10-07 12:17:4 Informatic 1 Firewall_ot NPI_10.6. Phase established
2004-10-07 12:17:4 Informatic 1 Firewall_ot NPI_10.6. INITIAL-CONTACT sent
2004-10-07 12:16:2 Informatic 0 Isakmp daemon started
2004-10-06 15:17:3 Informatic 0 Isakmp daemon shutdown
2004-10-05 13:05:2 Informatic 0 Isakmp daemon started
2004-10-05 12:55:3 Informatic 0 Isakmp daemon shutdown
2004-10-04 09:54:4 Informatic 0 Isakmp daemon started
2004-10-04 09:53:4 Informatic 0 Isakmp daemon shutdown
2004-10-01 10:48:5 Informatic 2 Firewall_ot NPI_10.6. Phase established
2004-10-01 10:00:5 Informatic 2 Firewall_ot NPI_10.6. Phase established
2004-10-01 10:00:5 Informatic 1 NPI_10.6. Firewall_ot INITIAL-CONTACT received
2004-10-01 10:00:5 Informatic 1 Firewall_ot NPI_10.6. Phase established
2004-10-01 10:00:5 Informatic 1 Firewall_ot NPI_10.6. INITIAL-CONTACT sent
2004-10-01 09:58:3 Informatic 0 Isakmp daemon started
2004-10-01 09:55:5 Informatic 0 Isakmp daemon shutdown
2004-10-01 09:55:4 Informatic 0 Isakmp daemon started
2004-10-01 09:55:4 Informatic 0 Isakmp daemon shutdown
2004-09-30 07:40:1 Informatic 1 NPI_F25 Firewall_ot Received Delete SA
2004-09-30 07:40:1 Informatic 2 NPI_F25 Firewall_ot Received Delete SA (SPI 0x0155d82b)
admin@10.6.4.2 (ro) 1 Hôtes 1 Utilisateurs authentifiés 0 tunnels VPN Alarmes: Majeure=0, mineure=0 Prêt

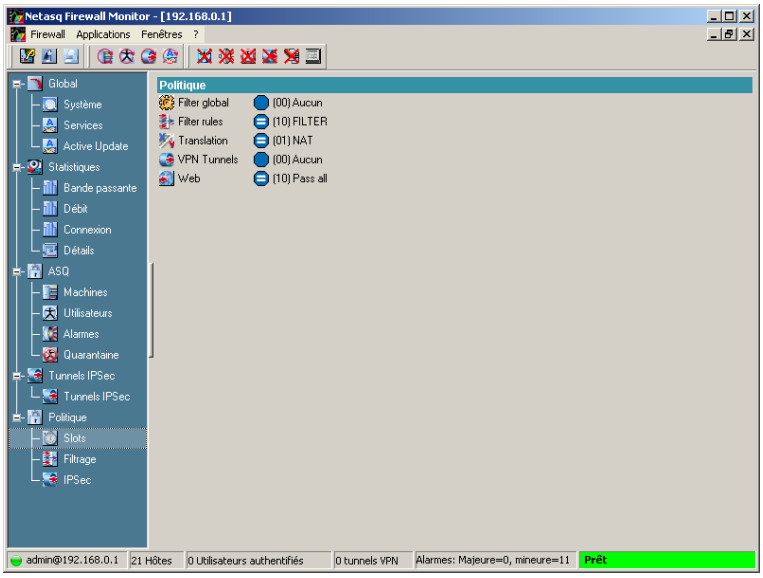
En cliquant sur l'onglet VPN, vous affichez les données suivantes :

Date Heure	Date et heure de génération de la ligne de logs.
Niveau d'erreur	message d'erreur.
Phase	phase de négociation de la SA.
Source	Adresse source de la connexion.
Destination	Adresse destination de la connexion.
Identité du correspondant	Identité du correspondant indiquée dans la configuration des clés pré-partagées dans le cas où le type d'identité spécifié n'est pas « Adresse IP ».
Message	Message concernant la tentative de mise en place d'un tunnel.

© Copyright NETASQ 2006

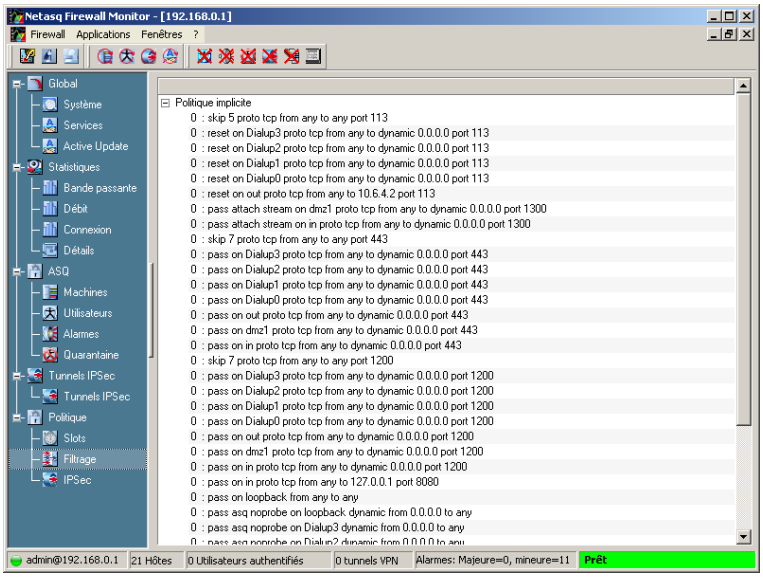
Le menu « Politique » est relatif à la politique de filtrage actuellement en place sur l'IPS-Firewall. Ce menu est divisé en deux sections.

Slots



Cette section affiche tous les slots de filtrage actuellement actifs parmi le slot de filtrage global, le slot de filtrage local, la translation d'adresse, la politique VPN et le filtrage d'URL.

Filtrage


Netasq Firewall Monitor - [192.168.0.1]
Firewall Applications Fenêtres ?
Global
Système
Services
Active Update
Statistiques
Bande passante
Débit
Connexion
Détails
ASQ
Machines
Utilisateurs
Alarmes
Quarantaine
Tunnels IPSec
Tunnels IPSec
Politique
Slots
Filtrage
IPSec
Politique implicite
0 : skip 5 proto tcp from any to any port 113
0 : reset on Dialup3 proto tcp from any to dynamic 0.0.0.0 port 113
0 : reset on Dialup2 proto tcp from any to dynamic 0.0.0.0 port 113
0 : reset on Dialup1 proto tcp from any to dynamic 0.0.0.0 port 113
0 : reset on Dialup0 proto tcp from any to dynamic 0.0.0.0 port 113
0 : reset on out proto tcp from any to 10.6.4.2 port 113
0 : pass attach stream on dmz1 proto tcp from any to dynamic 0.0.0.0 port 1300
0 : pass attach stream on in proto tcp from any to dynamic 0.0.0.0 port 1300
0 : skip 7 proto tcp from any to any port 443
0 : pass on Dialup3 proto tcp from any to dynamic 0.0.0.0 port 443
0 : pass on Dialup2 proto tcp from any to dynamic 0.0.0.0 port 443
0 : pass on Dialup1 proto tcp from any to dynamic 0.0.0.0 port 443
0 : pass on Dialup0 proto tcp from any to dynamic 0.0.0.0 port 443
0 : pass on out proto tcp from any to dynamic 0.0.0.0 port 443
0 : pass on dmz1 proto tcp from any to dynamic 0.0.0.0 port 443
0 : pass on in proto tcp from any to dynamic 0.0.0.0 port 443
0 : skip 7 proto tcp from any to any port 1200
0 : pass on Dialup3 proto tcp from any to dynamic 0.0.0.0 port 1200
0 : pass on Dialup2 proto tcp from any to dynamic 0.0.0.0 port 1200
0 : pass on Dialup1 proto tcp from any to dynamic 0.0.0.0 port 1200
0 : pass on Dialup0 proto tcp from any to dynamic 0.0.0.0 port 1200
0 : pass on out proto tcp from any to dynamic 0.0.0.0 port 1200
0 : pass on dmz1 proto tcp from any to dynamic 0.0.0.0 port 1200
0 : pass on in proto tcp from any to dynamic 0.0.0.0 port 1200
0 : pass on in proto tcp from any to 127.0.0.1 port 8080
0 : pass on loopback from any to any
0 : pass asq noprobe on loopback dynamic from 0.0.0.0 to any
0 : pass asq noprobe on Dialup3 dynamic from 0.0.0.0 to any
admin@192.168.0.1
21 Hôtes
0 Utilisateurs authentifiés
0 tunnels VPN
Alarmes: Majeure=0, mineure=11
Prêt

© Copyright NETASQ 2006

La section « filtrage » du moniteur récapitule la politique de filtrage active en regroupant les règles implicites, les règles de filtrage global et les règles de filtrage local.

Chaque ligne présentée se présente de la façon suivante :

<Identifiant du type de règle> : <Identifiant de la règle dans le slot> : <règle de filtrage>

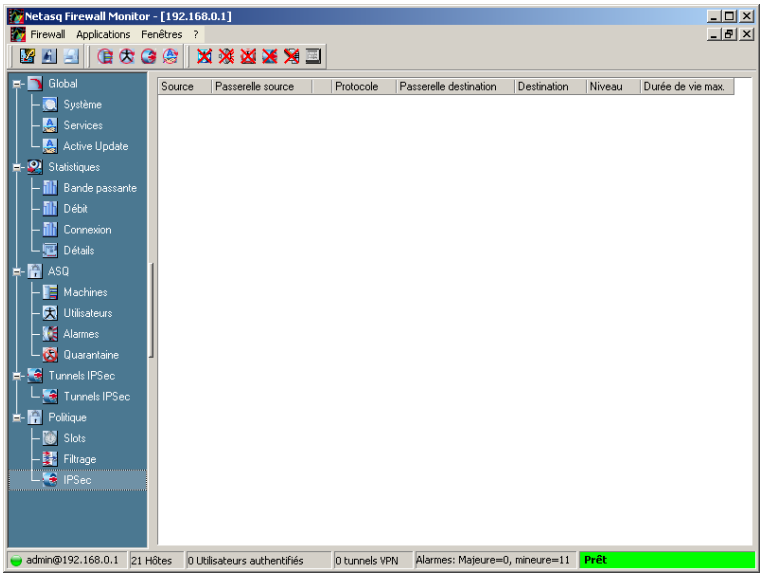
où :

► <identifiant du type de règle> peut être « 0 » s'il agit de règles implicites, « 1 » s'il s'agit du filtrage global et 2 s'il s'agit du filtrage local.

► <identifiant de la règle dans le slot> : dans le cas des règles implicites, cet identifiant est toujours « 0 ».

► <règle de filtrage> : règle de filtrage selon la grammaire NETASQ.

IPSEC



La section IPSec du menu « Politique » permet la visualisation de la configuration des différentes politiques de tunnels VPN IPSec définies dans le slot VPN actif. Il n'est pas nécessaire que ces politiques VPN soient réellement utilisées pour qu'elles soient affichées. Il est juste nécessaire que le slot VPN soit activé.

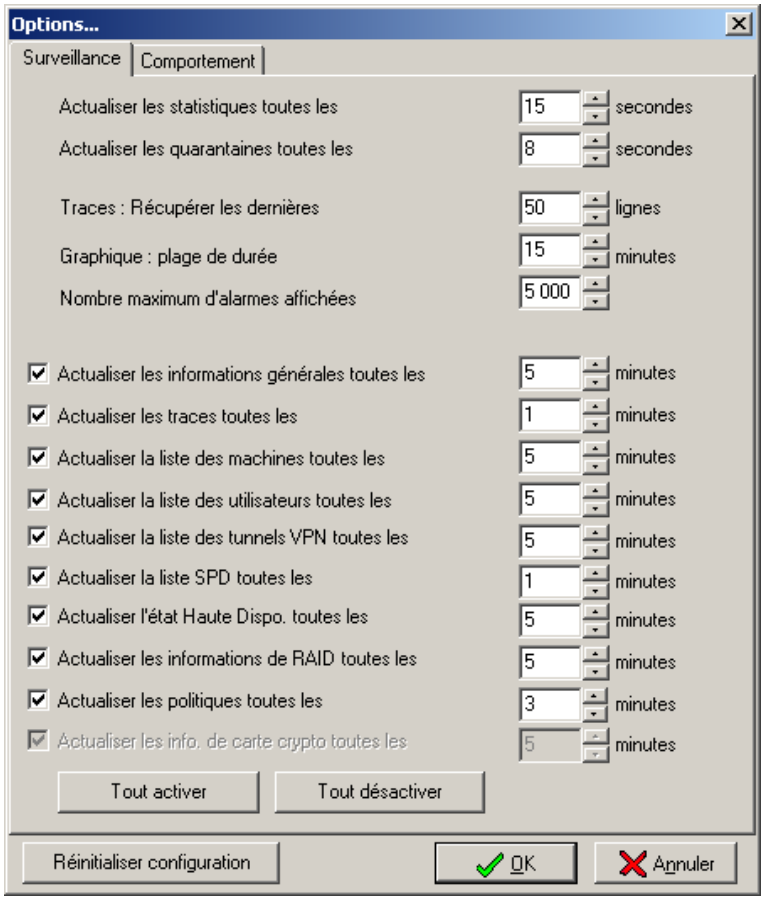
La grille de la section IPSec indique à chaque politique VPN configurée, les extrémités de trafic (les réseaux qui correspondent au travers du tunnel VPN IPSec), les extrémités de tunnels (les passerelles qui forment le tunnel VPN IPSec), le ou les protocoles autorisés à traverser le tunnel, le niveau de sécurité associé à ce tunnel (défini lors de la création du tunnel VPN IPSec en fonction des algorithmes de chiffrement et d'authentification) ainsi que la durée de vie maximale de la politique VPN configurée.

© Copyright NETASQ 2006

Section C

Options

© Copyright NETASQ 2006


Options...
Surveillance
Comportement
Actualiser les statistiques toutes les 15 secondes
Actualiser les quarantaines toutes les 8 secondes
Traces : Récupérer les dernières 50 lignes
Graphique : plage de durée 15 minutes
Nombre maximum d'alarmes affichées 5 000
Actualiser les informations générales toutes les 5 minutes
Actualiser les traces toutes les 1 minutes
Actualiser la liste des machines toutes les 5 minutes
Actualiser la liste des utilisateurs toutes les 5 minutes
Actualiser la liste des tunnels VPN toutes les 5 minutes
Actualiser la liste SPD toutes les 1 minutes
Actualiser l'état Haute Dispo. toutes les 5 minutes
Actualiser les informations de RAID toutes les 5 minutes
Actualiser les politiques toutes les 3 minutes
Actualiser les info. de carte crypto toutes les 5 minutes
Tout activer
Tout désactiver
Réinitialiser configuration
OK
Annuler

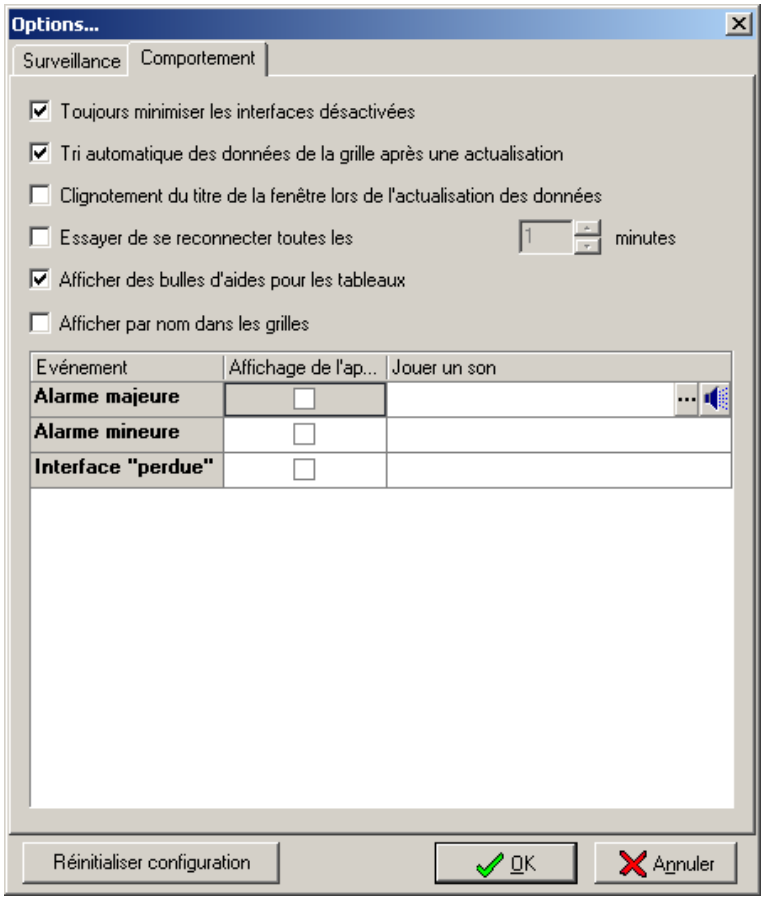
Vous accédez à cette fenêtre avec l'icône de la fenêtre du moniteur.

Vous pouvez configurer ici les temps de rafraîchissement de l'ensemble des informations contenues dans le monitor.

Vous pouvez configurer la période d'affichage des différents logs (en nombre de lignes) et aussi des différents diagrammes (en minutes).

Le bouton « Réinitialiser » permet de redéfinir la configuration des paramètres dans leurs valeurs par défaut.

© Copyright NETASQ 2006



Vous accédez à cette fenêtre avec l'icône de la fenêtre du moniteur.

Clignotement du titre de la fenêtre lors de l'actualisation des données

L'option fait clignoter le titre de la fenêtre lorsqu'un rafraîchissement de données à lieu.

Toujours minimiser les interfaces désactivées

L'option réduit automatiquement la fiche d'informations des interfaces désactivées (dans l'onglet Détails).

Tri automatique des données de la grille après une actualisation

L'option, désactivée par défaut, re-trie automatiquement l'ensemble de la grille (en fonction de la configuration de vos tris) lorsque vous rafraichissez les données affichées. Nous vous conseillons d'éviter de sélectionner cette option si la taille de la grille est conséquente sous peine de ralentissement important du Firewall Monitor.

Reconnexion auto. Après une déconnexion

L'option permet une reconnexion automatique du firewall Monitor sur le firewall après une déconnexion (reboot du firewall, …). Définissez un intervalle de temps entre chaque tentative de reconnexion.

Afficher les bulles d'aide pour les tableaux

Lorsque cette option est décochée, les infobulles affichées par le moniteur lors du parcours des grilles de traces n'apparaîssent plus.

© Copyright NETASQ 2006

Afficher le nom dans la grille

Lorsque le nom de l'objet est indiqué dans les traces, ce nom est affiché dans la grille. En décochant cette option, le nom n'est plus affiché et est remplacé par l'adresse IP associée à l'objet.

Evénements

Dans cette fenêtre vous choisissez aussi les actions à mener lorsqu'une alarme majeure ou mineure se déclenche ou lorsqu'une interface est inactive. Vous pouvez distinguer des actions différentes en fonction du type d'événement.

Les deux actions possibles à la réception d'événements en provenance du Firewall sont :

► **Affichage de l'application** : à la réception d'une alarme la fenêtre iconisée du moniteur s'ouvre et vient se placer devant les autres fenêtres ouvertes,

► **Jouer un son** : il faut alors préciser le fichier .WAV qui sera joué. L'icône permet d'écouter le son choisi.

Le bouton « Réinitialiser » permet de redéfinir la configuration des paramètres dans leurs valeurs par défaut.

Chapitre XIV

NETASQ Reporter et Reporter PRO

© Copyright NETASQ 2006

Le NETASQ REPORTER (dans sa version STANDARD et dans sa version PRO) est un autre module de la suite d'administration des firewalls NETASQ. Cet applicatif permet la visualisation des informations de logs, générées par les firewalls NETASQ.

Ces informations peuvent être utilisées pour analyser l'activité de votre réseau, l'accès à vos ressources informatiques, l'utilisation de l'Internet réalisée par les employés (sites WEB visités, utilisation de la messagerie...), afin de diagnostiquer les attaques informatiques repérées et bloquées par le firewall.

Les informations sont présentées sous forme de tableaux, permettant une analyse fine et détaillée, ou sous forme de graphiques, apportant une vision consolidée et globale des données.

Les fonctions d'audit du Firewall Reporter permettent à l'auditeur d'afficher les événements stockés dans chacun des fichiers de trace en effectuant :

► des sélections selon des périodes prédéfinies par rapport à la date courante (« aujourd'hui », « cette semaine », etc.) ou définies manuellement,

► des tris (croissants/décroissants) sur la valeur de chacun des champs des événements de sécurité enregistrés,

► des regroupements hiérarchiques en fonction de la valeur d'un ou plusieurs champs des événements de sécurité enregistrés.

Les logs analysés par le NETASQ REPORTER sont récupérés soit directement, à chaque requête, sur le firewall désiré, soit dans les fichiers SYSLOG alimentés par le service NETASQ (NETASQ SYSLOG). Dans ce dernier cas, les fichiers de traces sont stockés en local sur la machine d'administration, le NETASQ SYSLOG et le NETASQ REPORTER doivent être installés sur la même machine.

Le NETASQ REPORTER est disponible en deux versions : une version standard et la version professionnelle.

La version standard récupère les données désirées, à chaque requête, sur le firewall ou depuis des fichiers alimentés par le service NETASQ. La version professionnelle (présente dans l'Administration Suite PRO) utilise une base de données de type MySQL ou INTERBASE, en plus des fonctionnalités de la version standard.

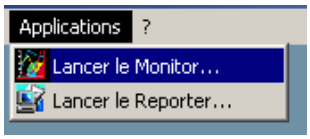
© Copyright NETASQ 2006

Section A

L’interface

© Copyright NETASQ 2006

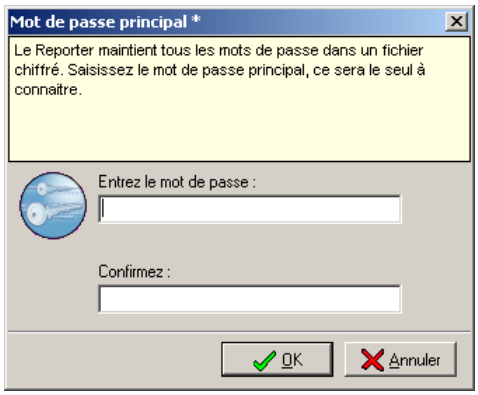
Pour utiliser le NETASQ REPORTER, lancez l'application à partir du menu « Démarrer » de Windows, par le chemin suivant : « Démarrer > Programmes > NETASQ > Administration Suite x.x > FIREWALL REPORTER » ou depuis votre Firewall Manager : « application > Lancer le Reporter ».



Au lancement de l'application Reporter par le menu « Windows », celui-ci vérifie l'existence d'un carnet d'adresses. Ce carnet d'adresses commun à toutes les applications NETASQ peut être chiffré ou pas. Si ce carnet d'adresses est chiffré ou si le carnet d'adresses n'existe pas encore, il y a une étape préalable à la connexion du reporter aux IPS-Firewalls.

Enregistrement préalable du mot de passe du carnet d'adresses

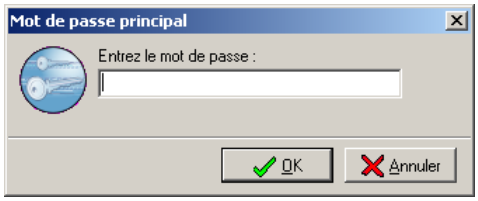
Si le carnet d'adresses n'existe pas encore, le Reporter demande l'entrée d'un mot de passe pour ce carnet d'adresses car par défaut celui-ci est chiffré (voir la section « Carnet d'adresses » pour comprendre les options du carnet d'adresses). Comme indiqué ce mot de passe sera le seul à retenir parmi tous les mots de passe de connexion nécessaires à la connexion sur le collector, la base de données et les futurs IPS-Firewalls qui seront enregistrés.


Mot de passe principal *
Le Reporter maintient tous les mots de passe dans un fichier chiffré. Saisissez le mot de passe principal, ce sera le seul à connaitre.
Entrez le mot de passe :
Confirmez :
OK
Annuler

Si un mauvais mot de passe est enregistré ou si le bouton « Annuler » est cliqué, le carnet d'adresses sera tout de même créé mais le chiffrement de celui-ci ne sera pas activé.

Connexion directe à un IPS-Firewall

Si le carnet d'adresses existe et qu'il est chiffré (voir la section « Carnet d'adresses » pour comprendre les options du carnet d'adresses), le mot de passe de ce carnet d'adresses est demandé avant toute connexion du reporter sur les différents IPS-Firewalls enregistrés.



Ensuite, le reporter affiche une grille d'affichage des traces et un popup de connexion permettant l'entrée des informations de connexion à un IPS-Firewall donné. Si le reporter est lancé depuis le Firewall Manager ou le Firewall Monitor, le reporter se connecte automatiquement à l'IPS-Firewall connecté au Firewall Manager ou Firewall Monitor.

© Copyright NETASQ 2006

Adresse	Adresse IP ou nom de machine du Firewall NETASQ sur le réseau interne.
Utilisateur	Nom d'utilisateur pour la configuration.
Mot de passe	Mot de passe pour l'utilisateur.
Lecture Seule	Connexion au firewall en mode lecture uniquement.

Si vous indiquez un nom de machine dans le champ « Adresse », ce nom doit être ajouté dans vos tables DNS ou dans le fichier hosts de la machine d'administration.

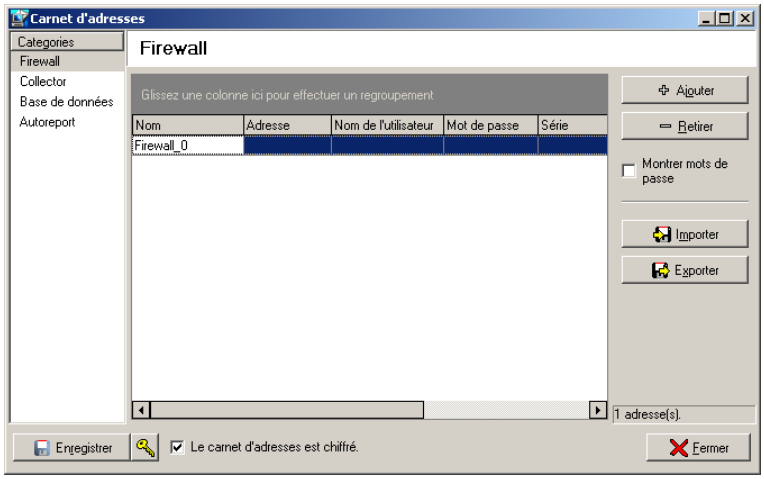
Attention, le Firewall NETASQ fait la différence entre les majuscules et les minuscules, aussi bien pour le nom d'utilisateur que pour le mot de passe.

Read Only permet une connexion en mode « lecture ». Ainsi vous pouvez vous connecter au firewall sans droits de modifications au moyen d'un compte possédant habituellement ces droits. Ceci permet de ne pas utiliser les droits de modifications si cela n'est pas nécessaire.

Cliquez sur « **Se connecter »** une fois ces champs renseignés. Vous pouvez vous connecter à plusieurs firewalls simultanément.

Carnet d'adresses

Le carnet d'adresses du reporter centralise tous les mots de passe pour l'accès aux différents modules (Firewall, Collector, Base de données, Autoreport).



Vous avez la possibilité de mémoriser les informations de connexion sur vos différents firewalls en cliquant sur l'icône située à côté du champ adresse du popup de connexion. Ces informations sont stockées sur le poste client où est installée l'interface. Elles peuvent être chiffrées si vous cochez l'option dans le menu « Logs > Options ». Dans ce cas, une clé de chiffrement vous est demandée. Indiquez pour chaque IPS-Firewall, un nom (ce champ est arbitraire et peut ne pas correspondre au nom de l'IPS-Firewall), une adresse IP, un mot de passe et un numéro de série.

Lorsque vous définissez un numéro de série pour un IPS-Firewall, ce numéro de série est ajouté à la liste des numéros de série connus la première fois que vous vous connectez à cet IPS-Firewall en utilisant le carnet d'adresses et cela sans qu'aucun message de confirmation n'apparaisse (voir « numéro de série inconnus **»).**

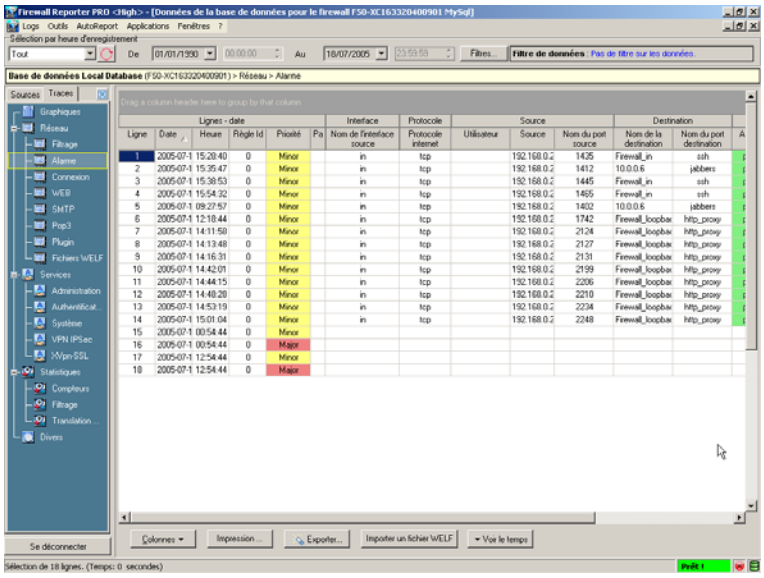
© Copyright NETASQ 2006

Il est fortement recommandé d'activer le chiffrement du carnet d'adresses pour des raisons de sécurité évidentes.

Une fois les informations entrées, vous pouvez les sauvegarder avec le bouton "Enregistrer". Pour ouvrir une session sur un des firewalls du carnet d'adresses, cliquez sur le nom de ce dernier puis sur le bouton "sélectionner" ou double cliquez sur ce même nom.

Attention, si vous modifiez l'option "chiffrer le carnet d'adresses" située dans les options générales, il faut enregistrer à nouveau le carnet pour prendre en compte les modifications.

Une fois que vous êtes connecté au firewall, la fenêtre principale du reporter s'affiche.



Elle est décomposée en quatre parties :

► une barre contenant une arborescence de menus ,

► une barre de sélection de date (permettant d'analyser uniquement les données de la période choisie),

► une zone d'affichage des résultats,

► une barre d'état.

Arborescence des menus

Cette arborescence est divisée en deux onglets :

► **Logs :** concentre toutes les opérations pour analyser les données,
► **Source :** permet de spécifier la source des logs visualisés (firewall, Syslog, Log Collector).

Onglet Logs

La section Logs contient cinq entrées :

► **Graphiques :** Permet de visualiser, sous forme de graphiques en ligne différents types d'information de l'IPS-Firewall (Indicateurs sécurité et système, utilisation du processeur, débit sur les différentes interfaces).

► **Réseau** : Cette section du reporter regroupe, sous forme de tableaux, toutes les traces générées par l'IPS-Firewall. Ces traces sont divisées en 8 tableaux : Filtrage, Alarmes, Connexion, WEB, SMTP, POP3, Plugin, Fichiers WELF.

► **Services :** Permet de visualiser, sous forme de tableaux, différents types de d'informations et de messages (actions réalisées sur le firewall manager, informations et erreurs d'authentification, informations et erreurs système ou informations et erreurs VPN)

© Copyright NETASQ 2006

► **Statistiques :** Permet de visualiser, sous forme de tableaux, différents types de statistiques (sur les règles de filtrage créées, les translations d'adresse, l'authentification ...).

► **Divers :** Permet de récupérer diverses informations sur les traces (quantité de traces sur le firewall et sur la base de données). A partir de cet écran, il est également possible de remettre à zéro les traces du firewall; on y trouve aussi la possibilité de générer un fichier contenant les adresses de base de tous les sites Internet consultés.

Remarque : Sélectionner une entrée déjà affichée permet de rafraîchir les données.

Onglet Sources

L'onglet Source permet la connexion aux différentes sources de compilation des traces fournies par NETASQ pour l'analyse des traces et des événements remontés par l'IPS-Firewall. Seul le Reporter PRO permet l'accès à tous les outils d'analyse de traces de NETASQ :

► **Firewall** : Connecté directement sur l'IPS-Firewall, cette méthode de récupération des traces permet de ne pas devoir utiliser d'outils de centralisation des traces. Mais il ne permet pas de pouvoir centraliser les traces de plusieurs IPS-Firewalls, souvent indispensable pour analyser un événement qui se propage sur plusieurs sites de l'entreprise. De plus cette méthode n'est disponible que pour les appliances disposant d'un disque dur. En effet sans ce disque dur, il ne peut y avoir d'enregistrement des traces directement sur l'IPS-Firewall.

► **Syslog** : Outil de récupération des logs, ce logiciel est disponible pour tous les produits. Il est indispensable aux appliances sans disque dur pour l'enregistrement de leurs traces. Par défaut il est configuré pour écouter sur le port UDP 514.

► **Collector** : Associé à une base de données capable d'agréger et de consolider les traces provenant de plusieurs IPS-Firewalls, le collector peut être associé à un syslog ou aller directement chercher les traces sur l'IPS-Firewall. L'administration de ce collector est réalisée dans le menu « outils », ce menu permet la connexion à la base de données.

► **Archives** : Permet l'accès à une archive préalablement réalisée. Le chemin d'accès à cette archive est configuré dans les écrans d'administration du collector à partir du menu « Outils ».

Connexion directe à l'IPS-Firewall

Le choix de connexion « Firewall » de l'onglet « Source » permet trois actions de connexion :

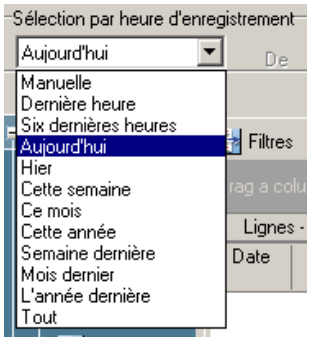
► **Nouveau** : En cliquant sur cette option, le carnet d'adresses s'ouvre automatiquement sur la liste des IPS-Firewalls déjà enregistrés. Cela permet l'enregistrement dans ce carnet d'adresses d'un nouvel IPS-Firewall.

► **Se connecter à** : En cliquant sur cette option, le popup de connexion apparaît et permet une connexion à un IPS-Firewall sans nécessiter son enregistrement.

► **Firewall_xx** : Enfin en plus des deux premiers choix, situés respectivement au début et à la fin de la liste des choix possibles, la listes des IPS-Firewalls déjà enregistrés est directement disponible. Elle permet ainsi l'ouverture rapide d'une connexion vers l'IPS-Firewall sélectionné.

© Copyright NETASQ 2006

Barre de sélection de date



Cette barre vous permet de définir la période sur laquelle vous désirez récupérer les données. Il existe des périodes prédéfinies :

► dernière heure,
► aujourd'hui,
► hier,
► cette semaine,
► ce mois,
► cette année,
► semaine dernière,
► mois dernier,
► l'année dernière,
► toutes les traces,
► sélection manuelle (vous pouvez définir une plage quelconque). Cette sélection permet de faire une extraction de données personnalisée.

Filtres (uniquement accessible avec la version pro)

Vous pouvez sélectionner des filtres à appliquer sur des colonnes et effectuer des recherches multicritères à partir du bouton de sélection (voir section Constructeur de Filtres).

Zone d'affichage des résultats

Dans cette zone apparaissent les données sous la forme sélectionnée (tableau, graphique...).

Le détail des tableaux et des graphiques est traité dans les chapitres suivants.

Barre d'état

Cette barre est constituée de 5 zones d'information :

► une zone de texte affichant en temps réel l'activité du Reporter,
► une barre de progression permettant d'estimer la durée d'une opération,
► une zone affichant l'état de l'application (un traitement est en cours ou non, réciproquement rouge ou vert),

© Copyright NETASQ 2006

► une icône indiquant l'état de la connexion avec le firewall,
► une icône indiquant l'état de la connexion avec la base de données.

La barre de menus de la fenêtre principale contient quatre entrées :

► Logs,
► Outils,
► Applications,
► Fenêtre,
► ?.

Menu Logs

Ouvrir	Permet de se connecter directement à un firewall via son protocole natif. *Remarque dans le cas d'un firewall F50, les informations sont récupérées depuis les fichiers générés par le SYSLOG (les traces du firewall sont récupérées par le service SYSLOG et transférées vers l'unité de stockage choisie).*
Carnet d'adresses	Accès au carnet d'adresses du Firewall Reporter.
Options	Configuration générale de l'application, de la base de données et des options de traces.
Quitter	Ferme toutes les connexions et quitte l'application.

Menu Outils

Gestionnaire de base de données	Permet d'accéder au gestionnaire de la base de données MySql, ainsi qu'à l'assistant d'archivage des traces. Ce menu n'est disponible que dans la version PRO du reporter.
Manager le collector	Permet d'obtenir des informations sur l'état du Log Collector et de relancer celui-ci. De plus toute la configuration du NETASQ Log Collector est réalisée dans ce menu du reporter PRO. Cette option n'est pas disponible pour la version STANDARD du Reporter. Toutefois s'il existe un Collector (Fonctionnalité Reporter PRO uniquement) installé sur une machine d'administration, le Reporter en version STANDARD est capable de s'y connecter.
Syslog UNIX	Si vous possédez des traces provenant d'un Syslog UNIX autre que le syslog NETASQ, l'assistant du menu « Syslog UNIX » permet de transformer ces traces en fichiers exploitables par le Reporter NETASQ.

© Copyright NETASQ 2006

Menu Applications

Le menu Applications permet une connexion aux autres applications de la suite d'administration NETASQ. Utiliser les deux raccourcis procurent l'avantage de ne pas devoir se ré authentifier sur ces deux applications.

Lancer le Manager	Permet l'ouverture du Firewall Manager de la suite d'administration NETASQ.
Lancer le Moniteur	Permet l'ouverture du Firewall Moniteur de la suite d'administration NETASQ.

Menu Fenêtre

Arranger les icônes	Permet d'organiser les icônes représentant les firewalls.
Cascade	Affiche en cascade les fenêtres connectées à des firewalls ou à des bases de données (version pro).
Disposition verticale	Permet d'organiser la disposition des fenêtres non réduites en icônes avec une disposition verticale.
Disposition horizontale	Permet d'organiser la disposition des fenêtres non réduites en icônes avec une disposition horizontale.

Menu ?

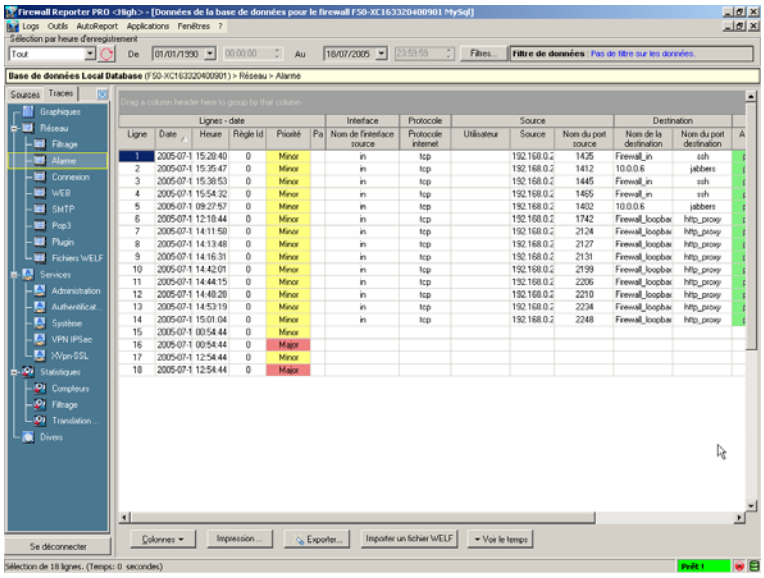
Aide	Affiche l'aide en ligne.
A propos	Affiche la boîte d'à propos, indiquant la version logicielle du NETASQ REPORTER. Dans la version professionnelle, nous retrouvons ici les informations sur la licence du REPORTER : version de la licence, nom de l'organisation, nom d'un contact, adresse email, identifiant unique pour le support.

Section B

Utilisation

© Copyright NETASQ 2006

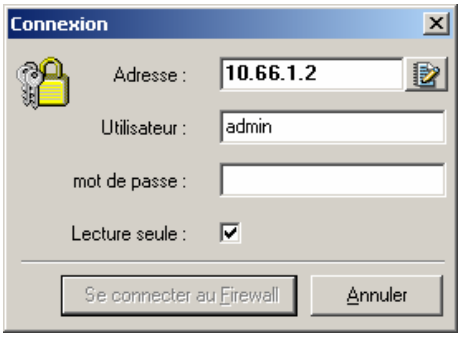
A partir de la fenêtre suivante, il est possible de choisir le type de consultation de données :



Dans la version Reporter Pro, vous pouvez soit vous connecter à un IPS-Firewall, soit utiliser les fichiers de traces stockés dans la base de données, soit consulter directement les fichiers Syslog.

Connexion à un IPS-Firewall

Pour vous connecter à un IPS-Firewall, utilisez l'option « Firewall » de l'onglet « Source » dans la barre de sélection de l'affichage. La fenêtre suivante s'affiche :



Adresse	Adresse IP ou nom de machine de l'IPS-Firewall NETASQ sur le réseau interne.
Utilisateur	Nom d'utilisateur.
Mot de passe	Mot de passe pour l'utilisateur.
Lecture seule	Connexion à l'IPS-Firewall en lecture seule.

Si vous indiquez un nom de machine dans le champ "Adresse", ce nom doit être ajouté dans vos tables DNS ou dans le fichier hosts de la machine d'administration.

Attention, l'IPS-Firewall NETASQ fait la différence entre les majuscules et les minuscules, aussi

© Copyright NETASQ 2006

bien pour le nom d'utilisateur que pour le mot de passe.

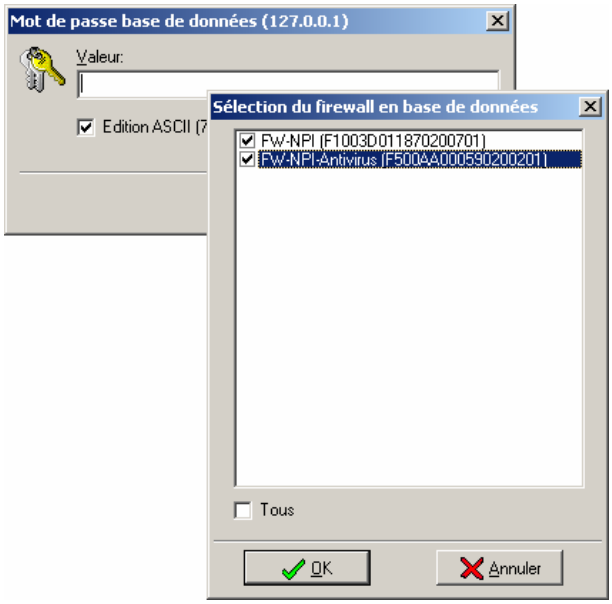
”Lecture seule” permet de se connecter en mode "lecture". Ainsi, vous pourrez vous connecter à l’IPS-Firewall sans droit de modification en utilisant un compte qui possède ces droits habituellement.

Cliquez sur "**Se connecter au Firewall**" une fois ces champs renseignés.

Vous pouvez vous connecter sur plusieurs IPS-Firewalls simultanément en ouvrant plusieurs fenêtres (avec le menu « Logs » > « Ouvrir »).

Connexion à la base de données Log Collector (Version PRO)

Pour vous connecter à la base de données, utilisez l’option « Collector » de l’onglet « Source » de la barre de sélection d’affichage. Les fenêtres suivantes s'affichent :



Renseignez le mot de passe de la base de données et cliquez sur "**OK**" .
Le mot de passe par défaut est « reporter ». Il est très fortement conseillé de modifier ce mot de passe dans le menu **Options** (voir dans la section Options).

Une fenêtre propose de sélectionner les IPS-Firewalls dans la base afin de visualiser les traces d’un ou plusieurs IPS-Firewalls. Vous pouvez également sélectionner tous les IPS-Firewalls de la liste en cochant l’option "**Tous**".

Lecture des traces du Syslog

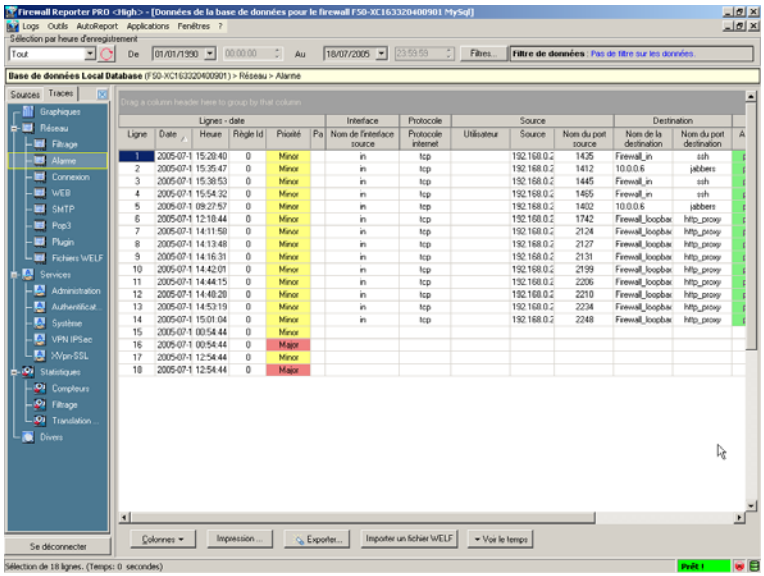
Pour analyser les traces récupérées par le Syslog, sélectionnez l’option « Syslog » de l’onglet « Source » de la barre de sélection d’affichage.

© Copyright NETASQ 2006

Le NETASQ REPORTER vous permet de visualiser les fichiers de traces sous forme de tableaux, ces fichiers sont divisés en deux sections « Fichiers » et « Contenu ». La section « Fichiers » fait référence aux traces générées par les règles de filtrage, la remontée des alarmes et les connexions. Tandis que la section « Contenu » fait référence aux traces générées par le filtrage de contenu.

Types de traces

Section « Réseau »



► **Filtre :** traces générées par les règles de filtrage. Pour obtenir ces traces, il faut qu'au moins une des règles de filtrage ait l'option "Tracer".

► **Alarmes :** alarmes remontées par le firewall.

► **Connexions :** informations sur toutes les connexions autorisées ayant transité au travers du firewall.

► **WEB :** traces des sites WEB consultés (plugin HTTP et proxy HTTP).

► **Mails (SMTP) :** traces des emails gérées par le proxy SMTP. Le proxy SMTP doit être activé pour que ces traces soient disponibles.

► **Mails (POP3)** : traces des emails gérées par le proxy POP3. Le proxy POP3 doit être activé pour que ces traces soient disponibles.

► **Plugin** : informations concernant les plugins activés sur votre firewall (sauf plugin HTTP).

► **Fichiers WELF importés (seulement sur la version PRO).**

Tri des colonnes

Les logs sont affichés dans un tableau possédant certaines propriétés facilitant la lecture des informations.

© Copyright NETASQ 2006

Tout d'abord, il est possible de trier les informations en fonction de leur type (alphabétique, date, octets...) par ordre croissant ou décroissant. Pour se faire, cliquez sur l'en-tête de colonne choisie. Une flèche pointant vers le haut ou le bas permet de constater l'effectivité du tri.

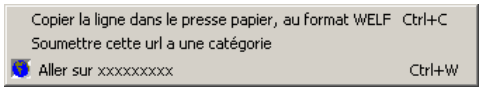
Un système de groupage, sous forme de nœuds, permet d'isoler les informations souhaitées. Une zone de "drop" est placée au dessus du tableau, vous pouvez y lire "Drag a column header here to group by that column". Pour regrouper les informations d'une colonne, sélectionnez le titre de la colonne et déplacez-le dans cette zone. Le tableau change alors d'aspect. La colonne ainsi groupée apparaît dans la zone de drop et le tableau affiche les valeurs résultant du groupage sous forme de nœuds. Un signe + apparaît devant les valeurs des groupes permettant de déplier les nœuds. Il est ainsi possible d'effectuer des regroupements à l'intérieur des groupes sans aucune limite.

Exemple : Lorsque vous sélectionnez l'affichage des logs d'URLs (Internet), il est possible de faire un regroupement par utilisateur puis par destination afin de mettre en évidence les consultations WEB réalisées par les utilisateurs internes.

Remarque : L'ordre des colonnes du tableau est personnalisable par le biais du mécanisme de « drag and drop ».

Menu contextuel

Dans chaque grille de traces du reporter, il existe un menu contextuel (on accède à ce menu en cliquant sur le bouton droit de la souris) qui permet le déclenchement rapide de certaines actions spécifiques. Trois options maximum sont définies pour le menu contextuel (en fonction de l'information sur laquelle on effectue un click droit) :


Copier la ligne dans le presse papier, au format WELF Ctrl+C
Soumettre cette url a une catégorie
Aller sur xxxxxxxxx Ctrl+W

► **Copier la ligne dans le presse papier et au format WELF :** Comme son nom l'indique cette option permet la réécriture au format WELF d'une ligne d'une grille de traces du Reporter vers le presse papier en vue d'une utilisation extérieure au Reporter.

► **Soumettre cette URL à une catégorie :** lorsqu'on accède au menu contextuel après avoir sélectionné une URL, cette option permet l'envoi de l'URL vers le formulaire de soumission d'URL sur le site WEB NETASQ.

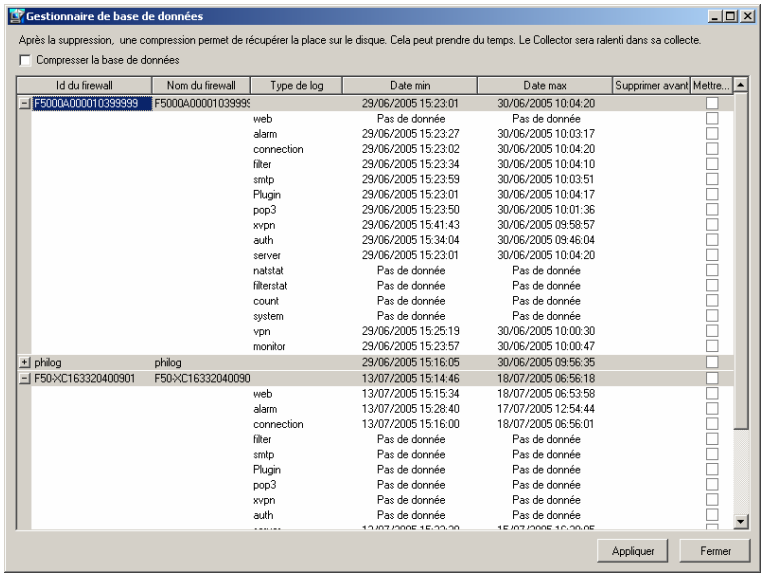
► **Allez sur xxxxxx :** lorsqu'on accède au menu contextuel après avoir sélectionné une destination, cette option permet une tentative de connexion en HTTP à cette destination.

© Copyright NETASQ 2006

Ce menu n'est uniquement disponible avec la version PRO du Reporter.

Base de données de travail

Le gestionnaire de la base de données permet de supprimer des traces dans la base de données de travail :


Gestionnaire de base de données
Après la suppression, une compression permet de récupérer la place sur le disque. Cela peut prendre du temps. Le Collector sera ralenti dans sa collecte.
Compresser la base de données
Id du firewall
Nom du firewall
Type de log
Date min
Date max
Supprimer avant
Mettre...
Appliquer
Fermer

Pour ouvrir le gestionnaire de la base de données, sélectionnez le menu « Outils », puis l'option « Gestionnaire de base des données » - « Base de données de travail ».

Pour supprimer des traces dans la base de données, sélectionnez une date pour marquer la fin de la sélection des traces à supprimer puis sélectionnez l'option « **Mettre à jour** » puis cliquez sur **« Appliquer »**. Une requête MySQL est envoyée à la base pour effacer les traces ainsi sélectionnées.

Veillez à ne pas supprimer les traces à la date précise où vous les avez archivées. En effet l'archivage de vos données est basé sur une date et une heure. Le système de suppression des traces étant basé uniquement sur une date inclusive, vous risquez de perdre certaines traces.

Compresser la base de données

Lorsque les traces sont supprimées dans la base de données, elles sont en réalité marquées « Supprimées » dans la base mais l'enregistrement de cette trace existe toujours ainsi la taille de la base de données ne diminue pas. Pour effectivement prendre en compte la suppression des lignes de traces, cochez l'option « Compresser la base de données ».

© Copyright NETASQ 2006

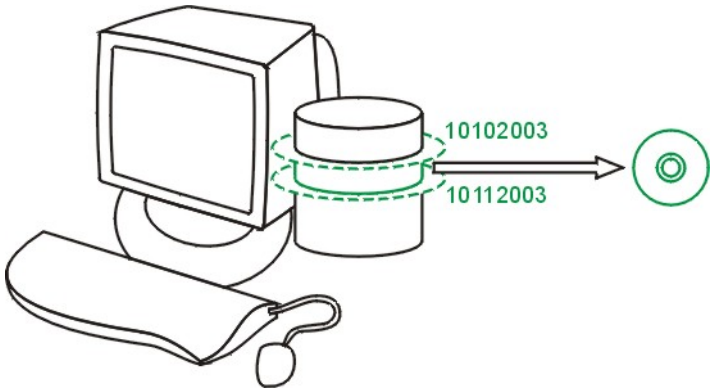
Création d'une archive

L'analyse et la gestion des traces générées par le trafic de votre réseau fait partie intégrante de la stratégie de sécurité de celui-ci. Suivant l'importance et le type de flux qui transitent sur ce réseau, cette tâche indispensable devient souvent fastidieuse voire laborieuse. Et cela de part le simple fait que les traces peuvent atteindre une taille très importante.

Une première étape vous permettant une meilleure gestion de ces traces est l'archivage. En effet les traces trop vieilles peuvent se révéler autant d'informations parasites lors de votre recherche de données particulières. Toutefois elles sont la mémoire de l'activité de votre réseau et vous ne devez absolument pas vous en séparer. Pour cela NETASQ vous propose de les archiver.

L'assistant d'archivage vous guide au travers de six étapes permettant une création rapide et simplifiée de vos archives de traces.

Principe de Fonctionnement

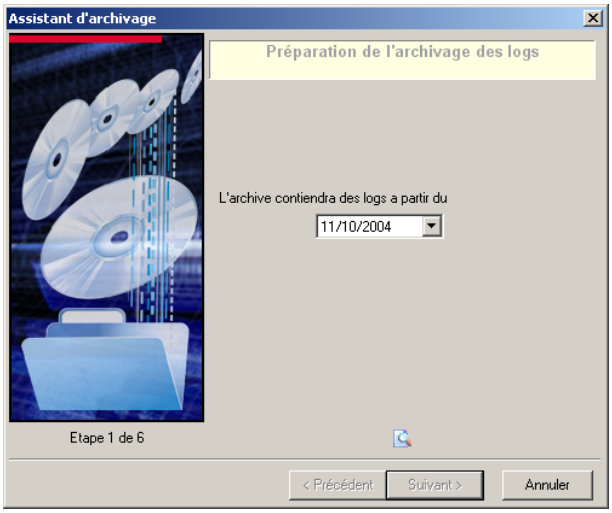


L'archivage des traces se présente de la façon suivante :

L'assistant vous demande de sélectionner une date de début d'archivage. Par défaut cette date se positionne au niveau de la date atteinte lors du dernier archivage (ou 01/01/2001 s'il s'agit du premier archivage).

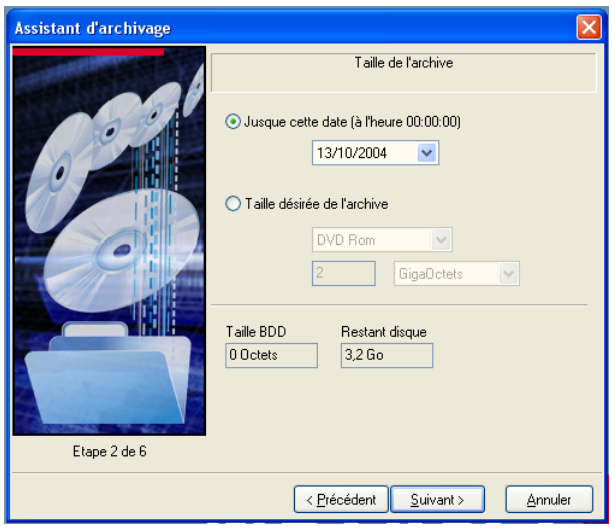
© Copyright NETASQ 2006

La fenêtre suivante vous permet d'indiquer cette date :



Puis vous devez sélectionner la taille de l'archivage que vous voulez créer. Cette taille correspond au type de média sur lequel les traces seront conservées. Deux formats par défaut ont été créés (CDROM et DVDROM) toutefois vous pouvez utiliser une taille personnalisée.

La taille que vous indiquez détermine la date de fin d'archivage. Cette opération nécessite une certaine durée; dépendant de la puissance de la machine sur laquelle est installé le Log Analyzer.

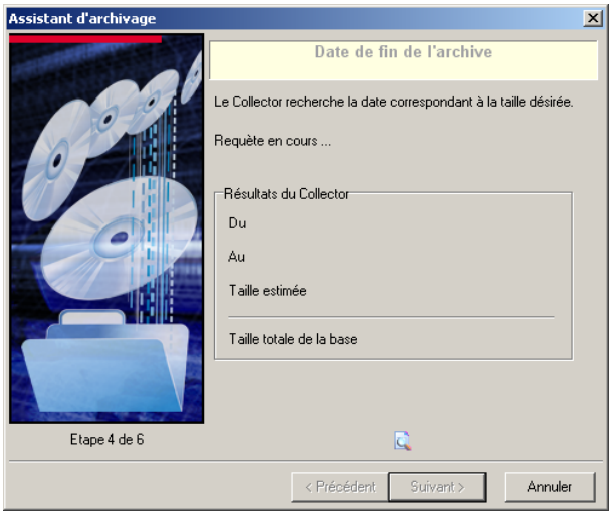


La fenêtre de l'étape 3 vous présente de manière succincte les actions qui seront effectuées lors des prochaines étapes.

Comme vous l'indique l'écran de l'étape 3, lors de l'archivage, les traces ne sont ni supprimées ni déplacées mais tout simplement copiées. La suppression des traces archivées doit être effectuée manuellement (voir section « Gestionnaire de la base de données »).

Assistant d'archivage
Création de l'archive
Cette étape devrait prendre du temps. Il s'agit d'un calcul d'une date finale pour générer l'archive de la taille projetée.
Puis d'une copie des logs de la base courante vers une nouvelle archive. Les logs ne sont ni déplacés ni supprimés mais copiés.
Le Collector stoppera la collecte des firewalls.
Etape 3 de 6
< Précédent
Suivant >
Annuler

Le calcul commence à l'étape 4 :



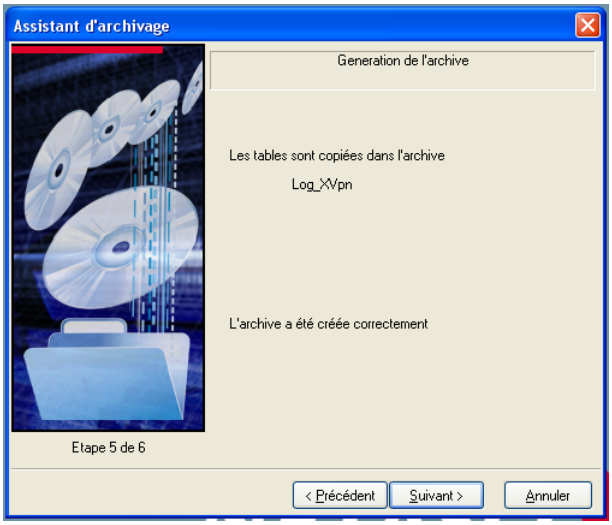
Lorsque le calcul est terminé, le Collector vous indique les résultats qu'il a obtenus :

- La date de début d'archivage (rappel de la sélection à l'étape 1),
- La date et l'heure de fin d'archivage,
- La taille estimée de l'archive,
- La taille totale de la base.

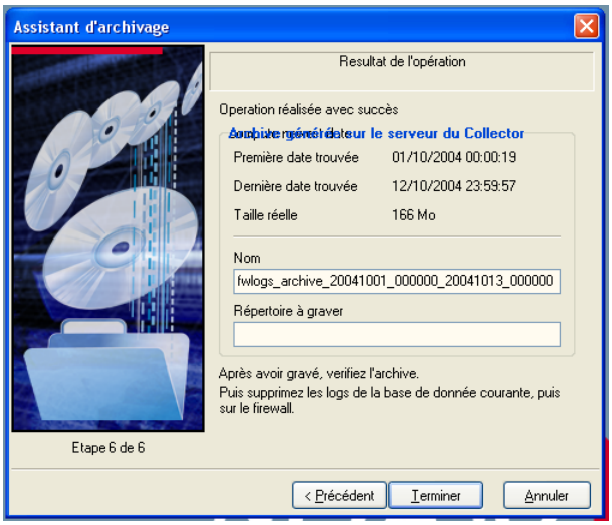
Ces informations sont très importantes si vous voulez supprimer les traces archivées. Toutefois plusieurs possibilités vous sont offertes pour retrouver ces informations :

- Lors d'un prochain archivage,
- A l'étape 6 de l'archivage,
- D'après le nom de l'archive générée.

© Copyright NETASQ 2006

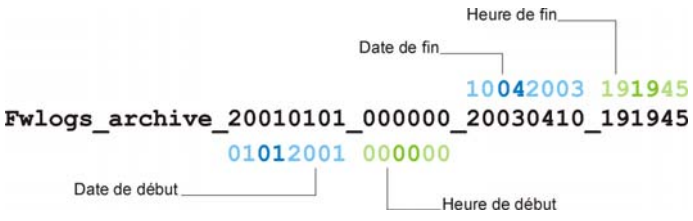


L'étape consiste à la création de l'archivage par le logiciel, si l'archive est réalisée correctement l'étape 6 termine la création de l'archive.



Enfin, l'étape 6 vous rappelle les informations d'archivage (début, fin, taille, nom…). Vous pouvez spécifier le nom de l'archive et le répertoire à graver.

On peut remarquer de quelle façon est défini le nom de l'archivage :

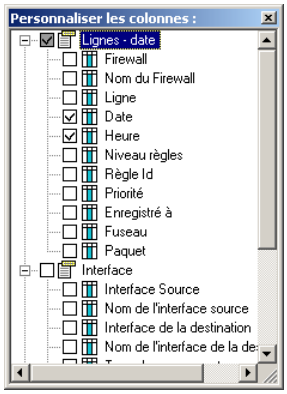


Les noms des colonnes suivantes correspondent aux informations qu'il est possible de consulter dans les traces. Ces colonnes sont regroupées par type de données pour former des en-têtes. Cette section décrit aussi la barre d'actions présente sous la grille de traces.

Les en-têtes

Ligne-date	Informations relatives à la ligne et à l'heure de la trace du paquet de données.
Interface	Informations relatives aux interfaces par lesquelles le paquet de données est passé.
Protocole	Informations relatives au protocole du paquet de données.
Source	Informations relatives à la source émettrice du paquet de données.
Destination	Informations relatives au destinataire du paquet de données.
Volume	Informations relatives au volume de données du paquet.
Action	Informations relatives aux volumes de données du paquet de données.
Opération	Informations relatives aux commandes effectuées dans l'utilisation des protocoles gérés par les plugins et les proxies.

Les colonnes



© Copyright NETASQ 2006

Ligne-date

Ligne	Numéro de la ligne de logs.
Priorité	Pour les alarmes, niveau de l'alarme (majeur ou mineur).
Date	Date de génération de la ligne de logs.
Heure	Heure de génération de la ligne de logs.
Nom Firewall	Nom du firewall.
Firewall	Numéro de série du firewall.
Règle Id	Identifiant de la règle.
Fuseau	Fuseau horaire du firewall.
Enregistré à	Heure d'enregistrement du log.
Niveau règles	Numéro correspondant à la classification des règles de filtrage (local ou global).
Paquet	Permet l'affichage du paquet ayant provoqué la remontée de l'alarme. Cette fonctionnalité doit être configurée dans le Moniteur de la suite d'administration.

Action

Action	Action de la règle de filtrage : « none », « pass », « block », « reset » respectivement aucune (règle qui n'a pas d'effet), passer, bloquer.
Message	Alarme.
Aide	Lien d'accès à l'explication de l'alarme remontée.
Alarme ID	Identifiant de l'alarme sur l'IPS-Firewall.
Répétition	Nombre de fois où l'alarme a été répétée dans l'intervalle de temps spécifié dans l'Administration Suite.
Nom de la règle	Cette colonne contient la valeur spécifiée dans le champ « Nom » de l'éditeur des règles de filtrage.
Classe	Classe à laquelle appartient l'alarme qui a été remontée.

Destination

Nom Destination	Adresse IP ou nom résolu de la destination.
Destination	Adresse IP de la destination.
Nom Port Destination	Nom du port de la destination.
Port Destination	Numéro du port de la destination.

Source

Nom Source	Adresse IP ou nom résolu de la source.
Source	Adresse IP.
Port Source	Numéro de port de la source.

© Copyright NETASQ 2006

Nom Port Source	Nom du port de la source.
Utilisateur	Nom de l'utilisateur authentifié.

Volume

Durée	Temps de la connexion.
Envoyé	Quantité de données envoyées.
Reçu	Quantité de données reçues.

Interface

Nom Interface Destination	Nom de l'interface de destination.
Mouvement	Mouvement du paquet.
Type Mouvement	Type de mouvement du paquet.
Nom Interface Source	Nom de l'interface source.
Interface Destination	Carte réseau de l'interface de destination.
Interface Source	Carte réseau de l'interface source.

Opération

Argument	Paramètre de l'opération.
Résultat	Code de retour de chargement.
Opération	Commande identifiée du protocole.
Catégorie	Catégorie à laquelle appartient l'URL ayant déclenchée la remontrée de traces.

Protocole

Protocole	Protocole de base.
Protocole Internet	Protocole Internet.
Groupe	Groupe de protocoles.

La barre d'actions

Filtre

Sélectionner cette option permet de constituer des filtres de données sur chaque colonne. Lorsque l'on active cette option, une flèche pointant vers la bas, apparaît à l'extrême droite de la colonne. La sélection d'une des valeurs pré-renseignées ou la saisie d'une valeur de votre choix restreint

automatiquement les données du tableau à celles correspondant au filtre sur la colonne sélectionnée.

Alors, la couleur de la flèche devient bleu marine, et en bas du tableau apparaît le filtre effectif. Une croix blanche permet de supprimer tous les filtres actifs en une seule fois.

Colonnes

Personnaliser	Les colonnes du tableau peuvent être déplacées, ôtées et ajoutées à souhait. Cette option permet de sélectionner les colonnes que l'on désire afficher. Il apparaît alors une fenêtre composée de deux onglets permettant de gérer les entêtes de colonne et les colonnes. Pou rajouter ou supprimer une colonne du tableau, il suffit de sélectionner le groupe de colonnes ou la colonne et de la glisser soit dans le tableau, soit dans la fenêtre surgissante.
Configuration par défaut	permet de restaurer l'affichage d'origine des colonnes.
Taille ajustée	permet d'ajuster la largeur des colonnes en fonction des valeurs.
Ajuster à l'écran	permet d'ajuster les largeurs des colonnes à la largeur de l'application.
Totalisation	Totalisation des volumes de paquets (envoyé, reçu, durée) pour l'ensemble des logs visualisés. Lorsqu'un tri (drag and drop d'une colonne) est effectué, un sous-total par tri est visualisable.

Imprimer

Grâce à cette option vous accédez à un menu de pré-visualisation avant impression.

Exporter

Il est possible d'exporter les données affichées afin de les exploiter dans d'autres environnements. Un assistant vous aide durant cette démarche. Celle-ci est décrite dans le paragraphe suivant.

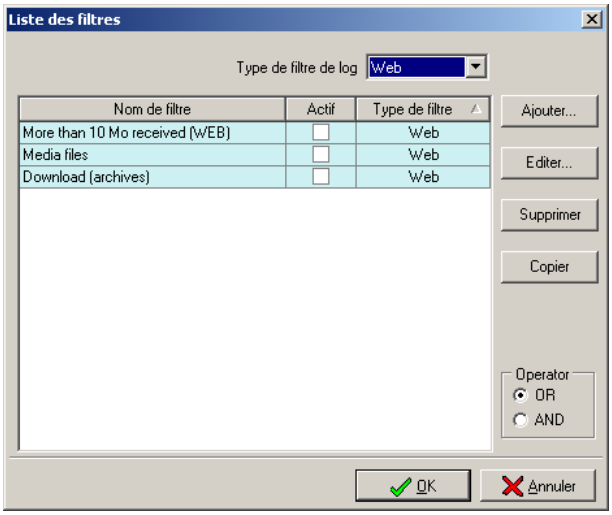
Importer un fichier WELF (version pro uniquement)

Voir le temps

Cette option vous permet de calculer automatiquement la date et l'heure des logs affichés dans le reporter et cela en fonction des différents fuseaux horaires suivant :

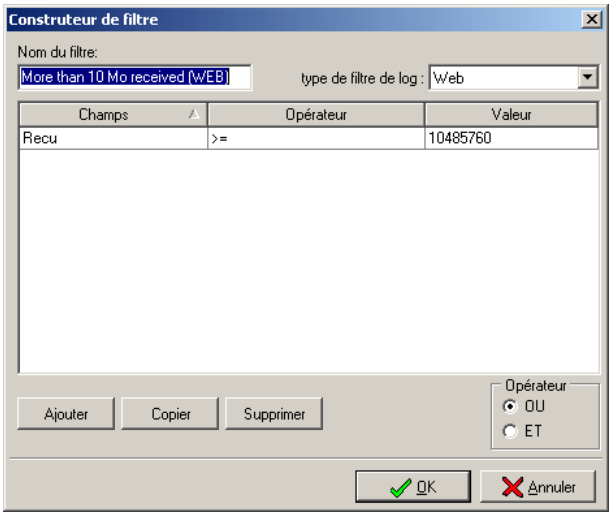
- ► le fuseau de votre station,
- ► le fuseau du firewall,
- ► GMT.

Le NETASQ Reporter Pro vous permet d'appliquer des filtres sur les colonnes et d'effectuer des recherches multicritères. Ces options de recherche profitent du langage SQL de la base de données. Cliquez sur le bouton de sélection « » dans la barre de sélection en haut à droite de la fenêtre active. Une nouvelle fenêtre s'ouvre :



Vous pouvez **Ajouter**, **Editer**, **Supprimer** ou **Copier** un filtre.

Vous pouvez construire des filtres simples ou multicritères grâce au constructeur de filtres.



Il est possible de sélectionner un type de filtre de traces afin d'appliquer la recherche sur un type de trace :

- ► Filtre,
- ► Alarmes,
- ► Connexions,
- ► Web,
- ► SMTP,

© Copyright NETASQ 2006

► Plugins,
► Fichiers chargés.

Pour chaque champ il est possible d'appliquer les opérateurs suivants :

► **= :** la valeur du champ est strictement égale,
► like : la valeur du champ contient une chaîne de caractères définie,
► **>= :** la valeur du champ est supérieure ou égale,
► **<= :** la valeur du champ est inférieure ou égale,
► **not like :** la valeur du champ ne contient pas une chaîne de caractères définie,
► **<> :** la valeur du champ est strictement différente,
► **start with :** la valeur du champ commence par une chaîne de caractères définie,
► **end with :** la valeur du champ se termine par une chaîne de caractères définie,
► **not start with :** la valeur du champ ne commence pas par la chaîne de caractères,
► **not end with :** la valeur du champ ne termine pas par la chaîne de caractères.

La colonne **Valeur** permet d'écrire la valeur qui peut être une chaîne de caractères ou une valeur numérique.

Il est possible d'ajouter des filtres et donc de créer des recherches multicritères à l'aide des boutons **Ajouter**, **Copier**, **Supprimer** et de l'**Opérateur** avec la valeur "**Ou**" ou la valeur "**Et**".

Une fois que le filtre est créé sélectionnez le bouton "Actif" pour activer le filtre, puis rafraîchir l'affichage des traces.

Un assistant vous guide dans l'exportation de vos données. Il est possible d'exporter les données sous 4 formats :

- CSV,
- HTML,
- XLS,
- XML.

Lorsque vous sélectionnez le format CVS, l'assistant vous propose de choisir un séparateur de champs.

Plusieurs choix sont disponibles :

- la tabulation,
- le point virgule,
- la virgule,
- l'espace,
- autre : un caractère (ou jeu de caractères) de votre choix.

Ensuite l'assistant vous propose de sélectionner les en-têtes de colonne et les colonnes à exporter au moyen d'un système de cases à cocher.

L'interface vous offre la possibilité de tout cocher ou tout décocher, de récupérer la sélection par défaut, de sauvegarder/restaurer votre sélection de colonnes. Chaque type d'export a sa propre sauvegarde. Une case à cocher permet d'automatiser cette opération.

Lorsqu'ensuite vous sélectionnez le bouton « Terminer », l'interface vous propose d'enregistrer le fichier généré dans le répertoire de votre choix. Ce répertoire est sauvegardé par type d'export.

Remarques

En version standard, seul l'export au format CSV est disponible.

Lorsque le Reporter se connecte directement sur un firewall, et que le nombre de lignes à récupérer sur le firewall excède 10000, un message de confirmation de téléchargement apparaît.

Lorsque le Reporter Pro se connecte à la base de données, et que le nombre de lignes à récupérer dans les tables excède 100.000, un message de confirmation de téléchargement apparaît.

Format des traces

Les traces sont au format WELF (WebTrend Enhanced Log Format).

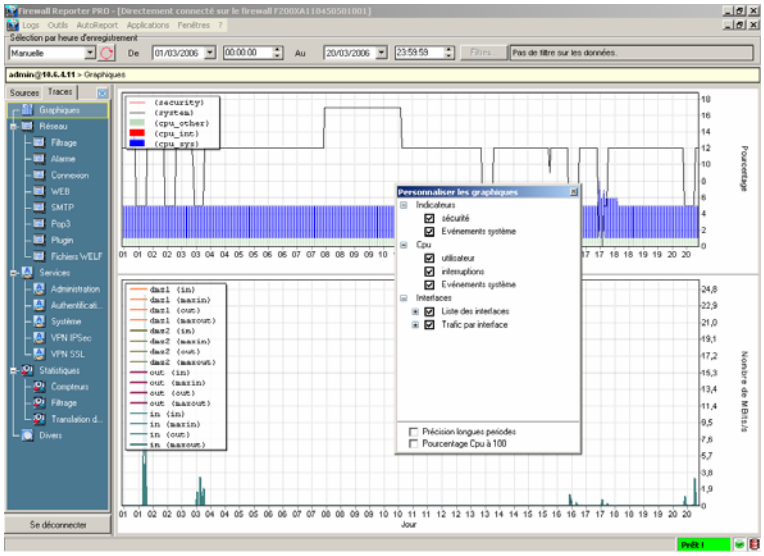
Descriptif des champs WELF

- **id (type indéterminé) :** identifiant du firewall ou son nom dans le cas où les logs du firewall sont ramassés par le Syslog,
- **line (type entier) :** numéro de la ligne de logs fw (type alphabétique) : numéro de série du firewall,
- **time (Log_Time, type date) :** date de la ligne de logs,
- **pri (type entier) :** priorité de l'événement (ref alarmes),
- **srcif (type alphabétique) :** interface source,
- **srcifname (type alphabétique) :** nom de l'interface,
- **dstif (type alphabétique) :** interface de destination,
- **dstifname (type alphabétique) :** nom de l'interface de destination,
- **movement (type entier) :** sens du mouvement (in to in, in to out, out to out, out to in),

© Copyright NETASQ 2006

► **MoveTypeMS (type entier) :** sens du mouvement (Serveur vers Serveur, Serveur vers Client, Client vers Client, Client vers Serveur),
► **ipproto (type alphabétique) :** protocole Internet,
► **proto (type alphabétique) :** protocole,
► **src (type alphabétique) :** adresse de la source (IPV6 ready),
► **srcport(type alphabétique) :** port de la source,
► **srcportname (type alphabétique) :** nom du port de la source,
► **srcname (type alphabétique) :** nom de la source,
► **dst (type alphabétique) :** adresse de destination (IPV6 ready),
► **dstport (type alphabétique) :** port de destination,
► **dstportname(type alphabétique) :** nom du port de destination,
► **dstname(type alphabétique) :** nom de destination,
► **user(luser, type alphabétique) :** ,
► **ruleid (type entier) :** identifiant de la règle de filtrage,
► **action (type chaîne) :** action reserved word for interbase,
► **msg (type alphabétique) :** ,
► **sent (type entier) :** quantité de données envoyées,
► **rcvd (type entier) :** quantité de données reçues,
► **duration(type réel) :** durée,
► **op(type alphabétique) :** opération,
► **result(type alphabétique) :** ,
► **arg(type alphabétique) :** argument (d'une page Internet).

L'activité des IPS-Firewalls peut être analysées par le reporter. En effet la section Graphiques du Reporter permet l'affichage des indicateurs Sécurité et Systèmes, l'utilisation du processeur de l'appliance ainsi que le débit sur les interfaces de l'appliances.



Indicateurs Sécurité et Systèmes

Les indicateurs système, ils sont attachés à la surveillance des événements relatifs aux interfaces Ethernet, à la charge du processeur de l'IPS-Firewall… Et les indicateurs sécurité, ils sont attachés à la surveillance des alarmes et des événements relatifs au noyau ASQ.

Les indicateurs systèmes concernent :

- ► les traces : indicateurs relatifs au remplissage de l'espace alloué aux traces,
- ► Ethernet : indicateurs relatifs à la connectivité des interfaces,
- ► CPU : indicateurs relatifs à la charge du processeur de l'IPS-Firewall,
- ► HA : indicateurs relatifs au dispositif de Haute Disponibilité, si elle est active,
- ► Serveur : indicateurs relatifs à certains serveurs critiques de l'IPS-Firewall.

L'affichage de ces indicateurs est basé sur la pondération des événements système les uns par rapport aux autres afin de présenter un état cohérent de l'IPS-Firewall.

Les indicateurs sécurité concernent :

- ► Alarmes mineures : indicateurs relatifs au nombre d'alarmes mineures,
- ► Alarmes majeures : indicateurs relatifs au nombre d'alarmes majeures,
- ► Mémoire ASQ : indicateurs relatifs au taux de remplissage de la mémoire ASQ.

L'affichage de ces indicateurs est basé sur la pondération des événements sécurité les uns par rapport aux autres afin de présenter un état cohérent de l'IPS-Firewall (les alarmes majeures auront plus de poids que les alarmes mineures).

Charge du CPU

Ce graphique représente la charge du processeur. On y distingue la charge imputable au noyau lui-même, la charge imputable aux processus lancés par l'utilisateur et la charge représentée par les échanges entre le noyau et les processus lancés par les utilisateurs.

Débit des interfaces

Cette section des graphiques représente l'utilisation de chaque interface de l'IPS-Firewall. Pour chaque interface, quatre informations sont données, la bande passante entrante à un instant donné,

© Copyright NETASQ 2006

la bande passante entrante maximale observée sur la période, la bande passante sortante à un instant donné et la bande passante sortante maximale observée sur la période.

Options des graphiques

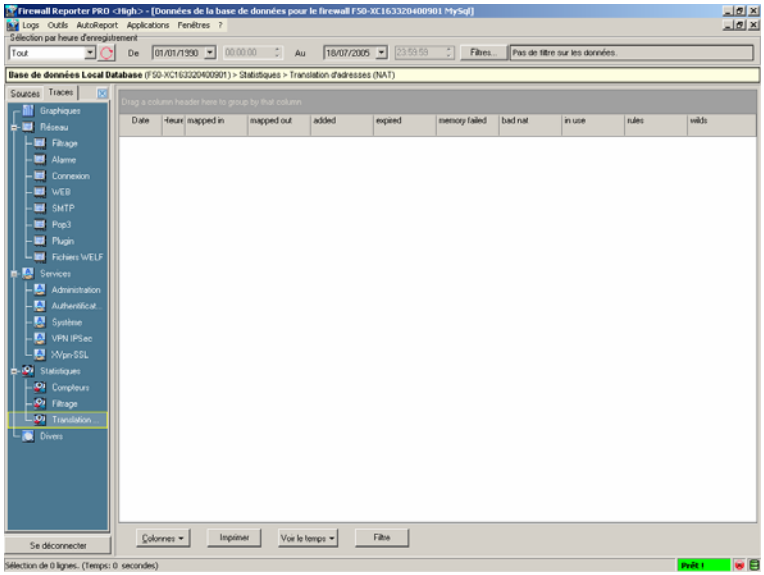
Précision longues périodes

Lorsque cette option est cochée tous les points de la période sont pris en compte. Or pour des périodes très longues, seul certains points significatifs sont pris en compte afin d'alléger l'affichage du graphique.

Charge du CPU à 100%

Lorsque cette option est décochée, l'échelle de l'affichage de la courbe de charge du processeur est dynamique. Ainsi si la charge du processeur est faible, les graphiques (l'échelle) sont adaptés de façon à être lisibles par l'administrateur. Dans le cas contraire, la valeur maximale de l'échelle reste toujours à 100% quelle que soit la valeur maximale observée jusqu'alors.

© Copyright NETASQ 2006



Il existe 3 analyses statistiques :

- ► Comptage,
- ► Filtre,
- ► Translation.

Le comptage

Correspond au nombre de fois qu'une règle a été utilisée. Pour que des informations soient affichées dans cette zone, il faur avoir activé l'option « Compter » dans les règles de filtrage.

Les filtres

Rule n	Nombre de fois qu'une règle a été activée.
SavedEvaluation	Evaluation économisée grâce à la technologie ASQ.
RealHostMem	Mémoire allouée à un ordinateur vu par le firewall.
HostMem	Mémoire allouée à l'adresse d'un ordinateur.
FragMem	Mémoire allouée aux fragments.
ICMPMem	Mémoire allouée aux paquets ICMP.
ConnMem	Mémoire allouée aux connexions.
Logged	Nombre de lignes de logs générées.
LogOverflow	Lignes de logs perdues.
Accepted	Paquets correspondant à la règle « pass ».

© Copyright NETASQ 2006

Blocked	Paquets correspondant à la règle « block ».
Byte	Quantité d'information traversant le firewall.
Fragmented	Quantité d'information fragmentée traversant le firewall.
TCPPacket	Nombre de paquets TCP traversant le firewall.
TCPByte	Totalité d'octets TCP traversant le firewall.
TCPConn	Nombre de connexions TCP traversant le firewall.
UDPPacket	Nombre de paquets UDP traversant le firewall.
UDPByte	Totalité d'octets UDP traversant le firewall.
UDPConn	Nombre de connexions UDP traversant le firewall.
ICMPPacket	Nombre de paquets ICMP traversant le firewall.
ICMPByte	Totalité d'octets ICMP traversant le firewall.

Remarque

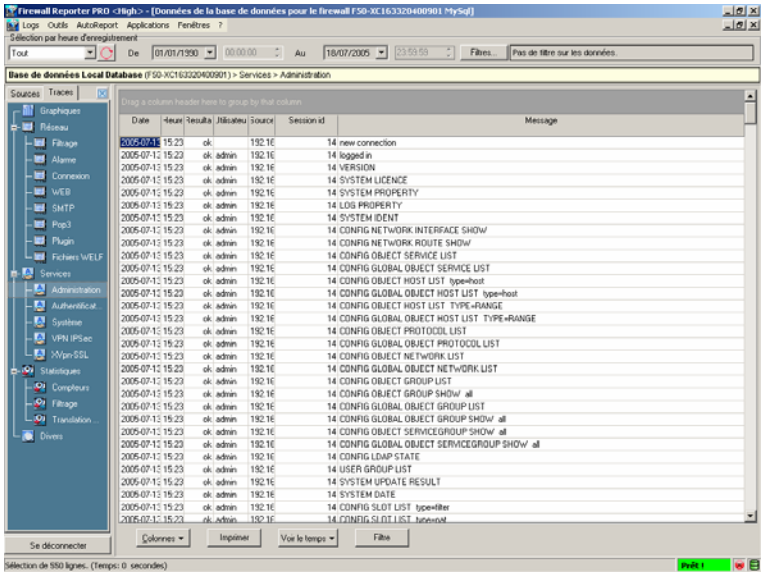
Lorsque l'on sélectionne une ligne d'un nœud développé, une explication apparaît dans la barre de bouton située en-dessous du tableau.

La translation

Active mapping	Translation active.
List of active MAP/Redirect filters	Liste des filtres de translation effectifs.
List of active sessions	Liste de sessions actives.
NAT statistics	Statistiques de translation.
Mapped	Nombre de connexions translatées.
Added	Nombre de connexions ajoutées.
expired	Nombre de connexions expirées.
Inuse	Nombre de connexions utilisées.
Rules	Nombre de règles de translation actives.
Wilds	Nombre de translations marquées « méta caractère ».

Remarque

La fréquence de calcul des statistiques est paramétrable depuis le Firewall Manager (cf Chapitre VIII Section A « configuration des traces ») uniquement pour les règles de filtrage incluant l'option « comptage »; cela est réalisé sur la période renseignée dans les options avancées du slot.



Il existe 5 services :

- ► Histo manager ;
- ► Authentification ;
- ► Système ;
- ► VPN ;
- ► VPN SSL.

L'historique du manager

Historique de toutes les commandes passées au firewall.

7 champs sont utilisés :

- ► Date ;
- ► Heure ;
- ► Utilisateur : identifiant de la connexion ;
- ► Source : adresse source de la connexion ;
- ► Session : format 00.0000. Les deux premiers chiffres correspondent au nombre de réinitialisations du firewall, les 4 suivants correspondent au nombre de connexions sur le firewall ;
- ► Status : message de retour de la commande ;
- ► Message : ligne de commande envoyée au firewall.

L'authentification

Historique des demandes d'authentification.

6 champs sont utilisés :

- ► Date ;

© Copyright NETASQ 2006

► Heure ;
► User : utilisateur demandant à être authentifié ;
► src : adresse de la demande d'authentification ;
► Method : méthode d'authentification ;
► Status : message d'erreur ;
► Message : Message de retour de la demande.

Système

Historique des messages liés aux services du firewall.

5 champs sont utilisés :

► Firewall : lorsque le reporter est connecté au collector, indique le firewall concerné par la ligne de traces affichée ;
► Date ;
► Heure ;
► Service : service associé au message ;
► Message : message associé au log.

VPN

Historique des événements concernant le VPN

13 champs sont utilisés :

► Firewall : lorsque le reporter est connecté au collector, indique le firewall concerné par la ligne de traces affichée ;
► Date ;
► Heure ;
► Error : message d'erreur ;
► Phase : phase de négociation de la SA ;
► Source : Adresse source de la connexion ;
► Destination : Adresse destination de la connexion ;
► Message : Message de concernant la tentative de mise en place d'un tunnel ;
► Utilisateur : identifiant de l'utilisateur (dans le cadre d'un tunnel anonyme) ;
► Cookie initiateur : identifiant « Initiateur » de la session de négociation en cours ;
► Cookie répondeur : identifiant « Répondeur » de la session de négociation en cours ;
► SPI IN : identifiant de la SA entrante ;
► SPI OUT : identifiant de la SA sortante.

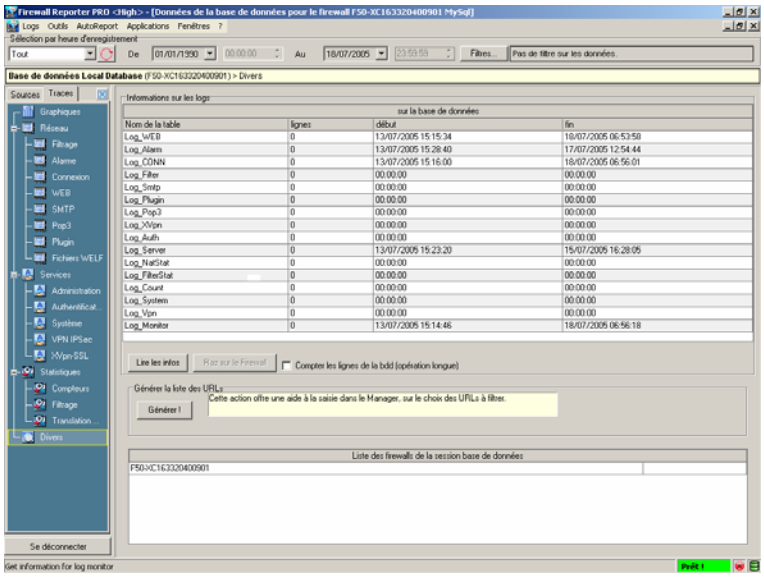
Historique des événements concernant le VPN SSL

11 champs sont utilisés :

► Firewall : lorsque le reporter est connecté au collector, indique le firewall concerné par la ligne de traces affichée ;
► Date ;
► Heure ;
► Résultat : résultat de la connexion VPN SSL au serveur sélectionné ;
► Port : port de connexion au serveur ;
► Nom du port : protocole généralement associé à un port donné ;
► Source : Adresse source de la connexion ;
► Destination : Adresse destination de la connexion ;
► Message : Message de concernant la connexion VPN SSL ;
► Utilisateur : identifiant de l'utilisateur ;
► Argument : informations complémentaires associées à la ligne de trace (page WEB contactée).

© Copyright NETASQ 2006

Le menu Divers permet de visualiser plusieurs informations.



La rubrique « Informations sur les logs »

Cette rubrique donne les informations sur le nombre de lignes de traces (sur la base de données et/ou sur le firewall).

La rubrique permet aussi de visualiser la différence entre les traces stockées sur l'IPS-Firewall et les traces stockées dans la base de données (dans le cas où une connexion de type « connexion au firewall et base de données simultanée » a été choisie). Un système de couleur surligne les lignes sur lesquelles un retard est constaté.

Afin de mettre à jour les informations, cliquez sur le bouton "Lire les infos".

Si vous possédez les droits de modification, une colonne supplémentaire apparaît permettant de sélectionner les logs à supprimer sur l'IPS-Firewall grâce au bouton « RAZ sur le firewall ». Les traces historisées sont alors effacées.

L'option « Compter les lignes de la BdD » vous permet d'afficher le nombre de lignes de traces disponibles dans chacune des catégories de traces de la base de données.Cette option est décochée par défaut car elle demande beaucoup de ressources lorsque la base de données est conséquente.

La rubrique « Générer la liste des URLs »

Génère dans un fichier HTML une liste des adresses Web visitées par les utilisateurs dans le cas où le filtrage URL est activé. Cette liste peut être utilisée pour renseigner les nouvelles URLs à filtrer, au niveau du Firewall Manager.

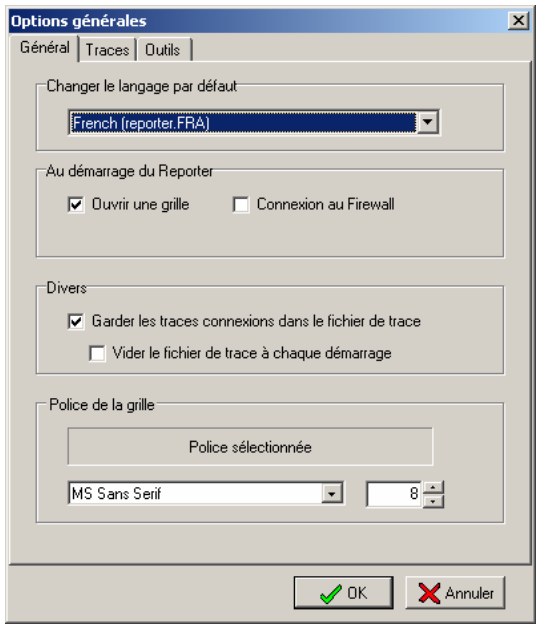
La rubrique « Informations sur le firewall » (si le Reporter est connecté à un IPS-Firewall)

Donne des informations sur l'IPS-Firewall auquel le Reporter Pro est connecté : identifiant du firewall (son numéro de série), nom du firewall, traces envoyées par le syslog (si les données sont récupérées via un Syslog), HA : état de la haute disponibilité.

La rubrique « Liste des firewalls de la session base de données » (si le Reporter est connecté uniquement à la base de données)

© Copyright NETASQ 2006

Dans le menu logs, vous avez accès à la configuration des options.



Onglet Général

Changer le langage par défaut : L'application REPORTER est une application multilingue. Choisissez la langue désirée pour l'interface graphique.

Au démarrage du reporter : Permet d'autoriser une connexion directe au firewall et d'ouvrir une grille de traces à l'ouverture de l'application.

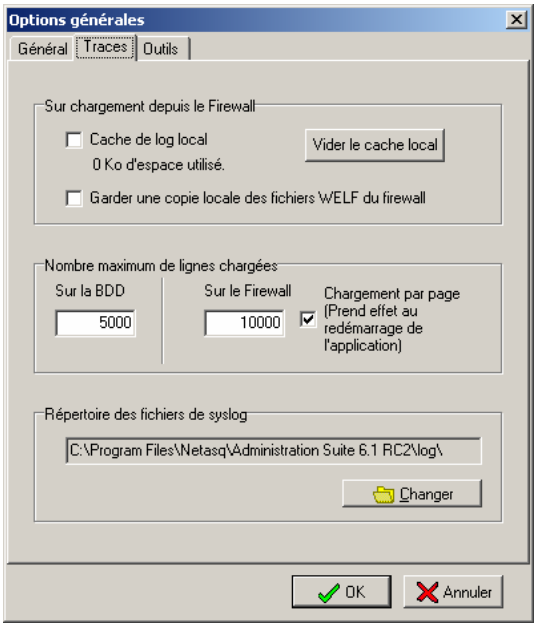
Garder les traces de connexions dans le fichier de trace : Permet de générer des traces concernant le comportement de l'application.

Vider le fichier de trace à chaque démarrage de l'application : Permet d'avoir un fichier au volume restreint et de ne conserver des traces d'activité que pour l'instance d'application en cours.

Police de la grille : Cette option permet de spécifier, la police et la taille du texte qui apparaît à l'intérieur de la grille de logs.

© Copyright NETASQ 2006

Onglet Traces



Sur chargement depuis le firewall

► **Cache log local** : cette option permet d'accélérer une recherche d'information de traces déjà effectuée. Les données ne sont plus rapatriées du Firewall lorsque cette option est sélectionnée et que les données ont déjà été rapatriées (les données sont alors stockées dans une base de données XML). Cette fonction n'est pas active lorsque l'on travaille sur la journée en cours.

► **Garder un copie locale des fichiers WELF du firewall :** Stocke en local tous les fichiers de traces téléchargés du firewall.

Nombre maximum de lignes chargées

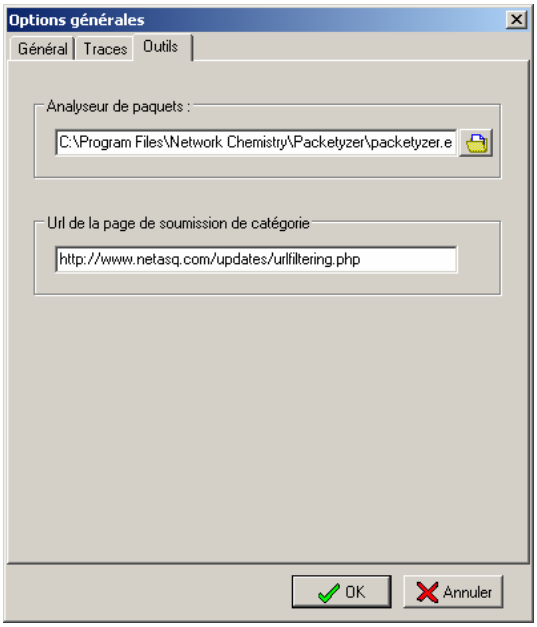
Cette option vous permet de spécifier le nombre maximal de lignes chargées pour la BDD ou pour le firewall. De plus afin de faciliter le chargement et la transformation des traces, celles-ci peuvent être affichées par page d'un maximum de 15000 lignes en cochant l'option « Chargement par page ». Si la période contient plus de lignes que le maximum autorisé alors les traces sont chargées en cache puis un système de navigation permet l'affichage par page d'un maximum de 15000 lignes à chaque fois (uniquement dans le cas de traces directement téléchargées depuis un IPS-Firewall).

Répertoire des fichiers de syslog

Le REPORTER récupère les traces dans les fichiers générés par le SYSLOG.

© Copyright NETASQ 2006

Onglet Outils



Analyseur de paquets

Lorsqu'une alarme se déclenche sur un IPS-Firewall NETASQ, il est possible de visualiser le paquet responsable du déclenchement de cette alarme. Pour cela il faut vous munir d'un outil de visualisation de paquets comme Ethereal ou Packetyzer… Spécifiez l'outil choisi dans le champ « Analyseur de paquets», celui-ci sera utilisé par le Reporter pour afficher les paquets malicieux.

URL de la page de soumission de catégorie

Les groupes d'URLs répertoriées et catégorisées ne sont pas éditables par les administrateurs des appliances UTM NETASQ. Toutefois certaines URLs peuvent s'avérer mal catégorisées ou non présentes dans la liste des URLs catégorisées par NETASQ. Pour ajouter une URL dans les listes d'URLs NETASQ, l'administrateur peut effectuer une soumission de cette URL sur le site WEB NETASQ.

L'URL de cette page de soumission est http://www.netasq.com/updates/urlfiltering.php. Pour effectuer une soumission l'administrateur possède deux choix : il se connecte directement sur le site WEB NETASQ pour spécifier manuellement cette URL ou dès que l'URL apparaît dans les tables du Reporter, il utilise le menu contextuel de la grille WEB du reporter pour que la soumission s'effectue automatiquement. Pour cela, il est nécessaire de spécifier l'URL de soumission dans le champ « URL de la page de soumission de catégorie » du Reporter.

© Copyright NETASQ 2006

Section C

NETASQ Log Collector (Version PRO)

© Copyright NETASQ 2006

Présentation

Le NETASQ Log Collector est un utilitaire chargé de récupérer toutes les traces stockées sur les équipements NETASQ ou collectées par un NETASQ Syslog et de les stocker dans une base MySQL ou Interbase.

© Copyright NETASQ 2006

Le NETASQ Log Collector est installé en tant que service : « **Fw LogCollector** ». Ce mode procure l'avantage de tourner de façon totalement transparente pour l'utilisateur (en tâche de fond). De plus, le service continue de fonctionner même sans ouverture de session Windows.

Uniquement sous Windows NT, 2000 ou XP.

Procédure d'installation du service

Le service Log Collector est installé automatiquement à l'installation du NETASQ Log Collector inclus dans le NETASQ Log Analyzer. Il est cependant possible de l'installer en lançant un exécutable se trouvant dans le menu « Démarrer » - « Programmes » -« NETASQ » - « Log analyzer <version> » - « **Services » - « Installer » – « lancer le Collector ».**

Sinon, la procédure complète est la suivante :

1. Ouvrez une invite de commandes DOS,
2. Placez-vous sur le répertoire NETASQ de votre disque dur (en principe : c:\Program Files\NETASQ\LogAnalyzer<version>),
3. Tapez la commande d'installation suivante : F*wLogCollector.exe /INSTALL /SILENT,*
4. Tapez la commande de démarrage du service : *NET START svcFwLogCollector.*

Une fois installé, le service sera redémarré à chaque reboot même si aucune session n'est ouverte.

Procédure de désinstallation du service

Le service Log Collector peut être désinstallé à l'aide d'un exécutablese trouvant dans le menu « Démarrer » - « Programmes » - « NETASQ » - « Log analyzer 1.0 » - « Services » -« **Arrêter » – « retirer le Collector ».**

Sinon, la procédure complète est la suivante :

1. Ouvrez une invite de commandes DOS,
2. Tapez la commande d'arrêt du service suivante : *NET STOP svcFwLogCollector,*
3. Placez-vous dans le répertoire NETASQ de votre disque dur (en principe C:\Program Files\NETASQ\LogAnalyzer 1.0),
4. Tapez la commande de désinstallation du service : *FwLogCollector.exe /UNINSTALL /SILENT,*

Il est recommandé d'arrêter et de redémarrer le service MySql à l'aide de l'outil de gestion des services inclus avec Windows NT, 2000 et XP.

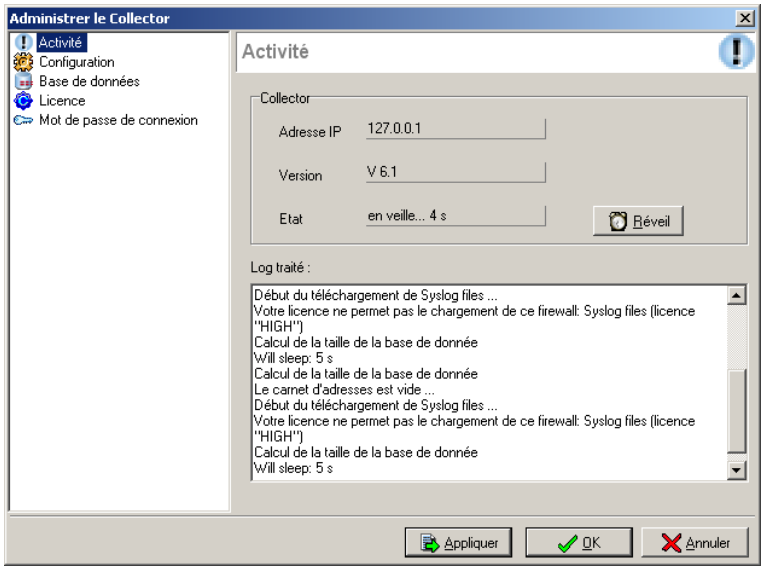
© Copyright NETASQ 2006

La configuration du NETASQ Log Collector est réalisée dans le Reporter PRO. Pour cela vous devez vous rendre dans le menu « outils » -« Administrer le collector » du Reporter PRO.

Si une fenêtre du Reporter PRO est ouverte lorsque vous sélectionnez le sous-menu « manager le collector », un message vous demandant de fermer toutes les fenêtres existantes apparaîtra.

Connexion au Log Collector

La connexion au Log Collector est transparente. En effet toutes les informations sont enregistrées dans le carnet d'adresses. Un mot de passe de connexion au Collector existe par défaut mais ces informations sont automatiquement enregistrées dans le carnet d'adresses. Il est possible de modifier ce mot de passe mais il est nécessaire que le carnet d'adresses soit modifié en conséquence. En cliquant sur le menu « Administrer le collector », le menu de configuration du Collector apparaît donc directement (sauf s'il existe plusieurs collectors différents configurés dans le carnet d'adresses) :


Administrer le Collector
Activité
Configuration
Base de données
Licence
Mot de passe de connexion
Activité
Collector
Adresse IP
127.0.0.1
Version
V 6.1
Etat
en veille... 4 s
Réveil
Log traité :
Début du téléchargement de Syslog files ...
Votre licence ne permet pas le chargement de ce firewall: Syslog files (licence "HIGH")
Calcul de la taille de la base de donnée
Will sleep: 5 s
Calcul de la taille de la base de donnée
Le carnet d'adresses est vide ...
Début du téléchargement de Syslog files ...
Votre licence ne permet pas le chargement de ce firewall: Syslog files (licence "HIGH")
Calcul de la taille de la base de donnée
Will sleep: 5 s
Appliquer
OK
Annuler

Par défaut le Log Collector et le Reporter PRO sont installés sur la même machine donc l'adresse de connexion est 127.0.0.1.

Par défaut le service Collector est en écoute sur le port 1380. N'oubliez pas de spécifier ce port de connexion dans la configuration du Collector si vous modifiez celui-ci.

Le menu de configuration du Log Collector est divisé en deux parties :

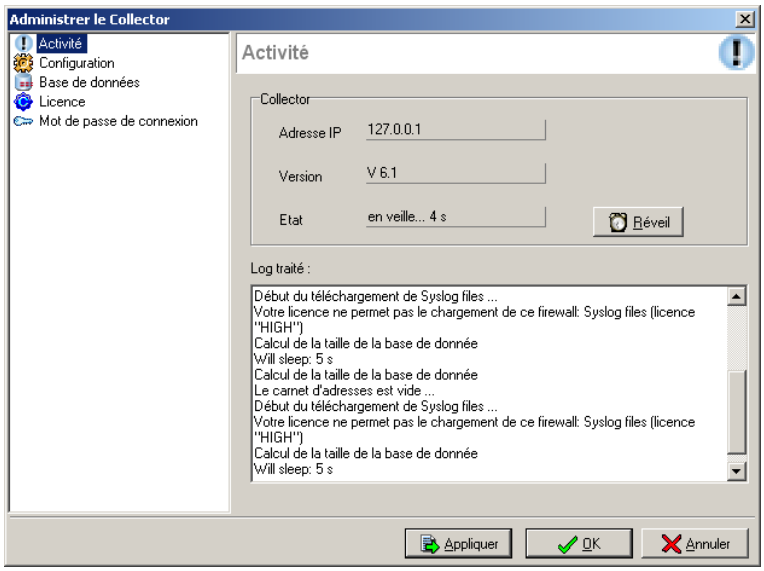
- A gauche un arbre présentant les diverses fonctionnalités du menu Log Collector,
- A droite les options configurables.

Le menu de configuration du Log Collector est composé des sous menus suivants :

- **Activité** : cet écran présente une visualisation de l'activité du NETASQ Log Collector,

© Copyright NETASQ 2006

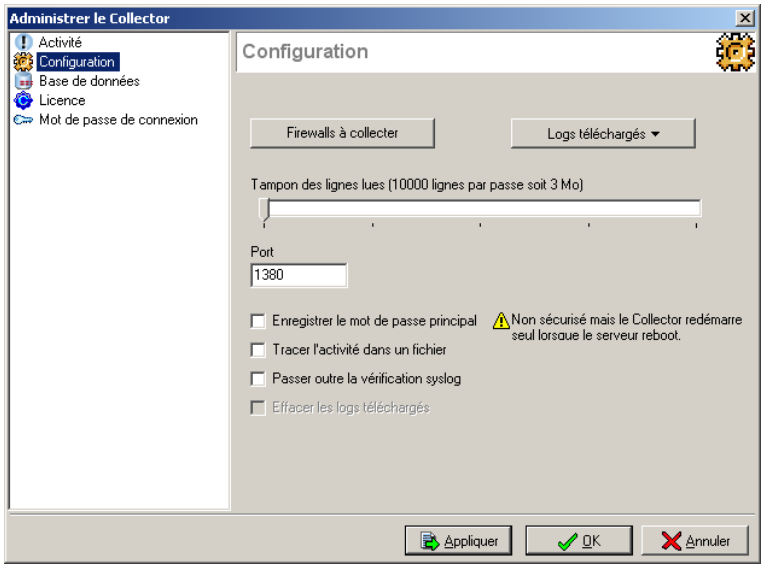
► **Configuration** : ce menu vous permet la configuration du Collector,
► **Base de données** : menu permettant la modification des mots de passe de la base de données,
► **Licence** : cet écran est utilisé pour l'insertion de nouvelles licences,
► **Mot de passe de connexion** : cet écran est utilisé pour la modification des mots de passe de connexion principal.


Administrer le Collector
Activité
Configuration
Base de données
Licence
Mot de passe de connexion
Activité
Collector
Adresse IP
127.0.0.1
Version
V 6.1
Etat
en veille... 4 s
Réveil
Log traité :
Début du téléchargement de Syslog files ...
Votre licence ne permet pas le chargement de ce firewall: Syslog files (licence "HIGH")
Calcul de la taille de la base de donnée
Will sleep: 5 s
Calcul de la taille de la base de donnée
Le carnet d'adresses est vide ...
Début du téléchargement de Syslog files ...
Votre licence ne permet pas le chargement de ce firewall: Syslog files (licence "HIGH")
Calcul de la taille de la base de donnée
Will sleep: 5 s
Appliquer
OK
Annuler

Activité

L'écran de visualisation de l'activité est divisé en trois parties :

► **Collector** : Cette partie vous informe sur les propriétés du Collector, son adresse, sa version, son état. Le bouton « réveil » vous permet de le relancer lorsqu'il est en veille,
► **Log traité** : Donne des informations sur le traitement des traces par le Log Collector
► **Reçu du LogCollector** : Cette section donne des informations remontées par le Log Collector.



Dans ce menu il est possible de configurer plusieurs paramètres :

► **Tampon des lignes lues** : il est possible de régler la taille du tampon mémoire utilisée par le NETASQ Log Collector pour rapatrier les traces, avant injection dans la base de données. Le minimum est de 3 Mo soit 10.000 lignes de traces, le maximum est de 15 Mo soit 50.000 lignes de traces.

► **Port** : spécifiez le port d'écoute du NETASQ Log Collector. Par défaut le port d'écoute est configuré à 1380.

► **Enregistrer le mot de passe principal :** permet de ne pas avoir à renseigner le mot de passe pour lancer le Collector. Il est fortement déconseillé de cocher cette case.

► **Tracer l'activité dans un fichier** : lorsque cette option est activée, toutes les opérations et les messages d'erreur du NETASQ Log Collector sont stockés dans un fichier. Ce fichier se trouve dans le répertoire des fichiers NETASQ Log Analyzer (en principe C:\Program Files\NETASQ\Log Analyser 1.0\) et se nomme logcollector.log.

► **Effacer les traces téléchargées** : permet de supprimer les traces sur l'IPS-Firewall lorsque celles-ci ont été stockées dans la base de données.

Firewalls à interroger

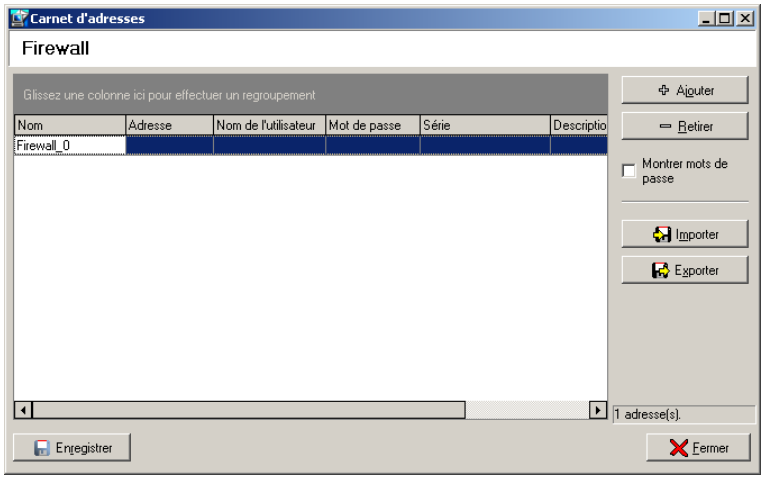
Afin que le NETASQ Log Collector puisse se connecter aux IPS-Firewalls pour télécharger les traces contenues sur ceux-ci, il faut créer un utilisateur qui aura des droits de lecture sur les traces, renseigner les paramètres de connexion des IPS-Firewalls pour lesquels on désire récupérer les traces, dans le carnet d'adresses (si vous possédiez précédemment un NETASQ Log Analyzer, vous pouvez récupérez le carnet d'adresses du Log Analyzer en copiant le fichier AddrScan.dat dans le répertoire d'installation du Reporter PRO). Il faut donc :

1 – Créer un utilisateur quelconque à l'aide du Firewall Manager sur chaque IPS-Firewall (voir aide en ligne du Firewall Manager), et attribuer à cet utilisateur des privilèges d'administration sur l'IPS-Firewall : **« Privilèges minimum pour le Log et Monitor »**.

2 – Renseigner l'adresse IP ainsi que le login et le password de l'utilisateur précédemment créé dans le Carnet d'adresses du NETASQ Log Collector.

Le carnet d'adresses se présente de la manière suivante (il est accessible via le bouton « Firewalls à interroger ») :

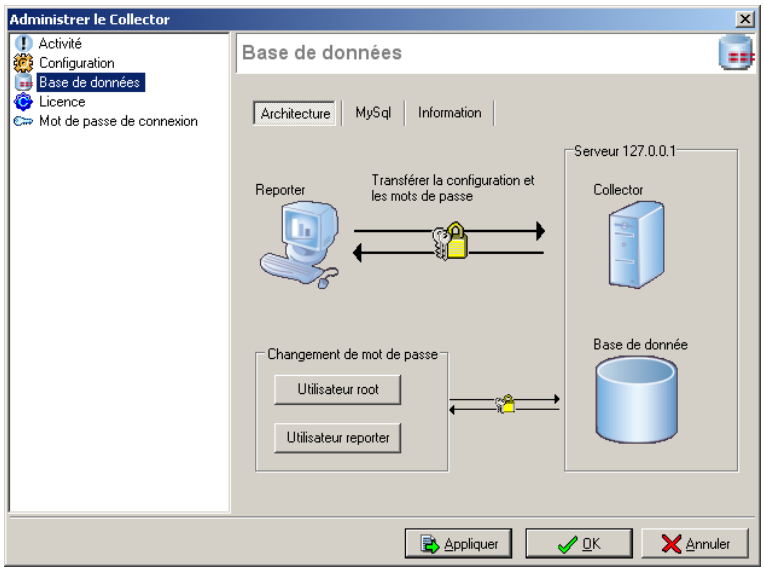
© Copyright NETASQ 2006



Lorsque le carnet d'adresses est enregistré les données sont chiffrées en AES sur votre machine. Pour prendre en compte ces modifications vous devez envoyer ces informations au collector au moyen du bouton « Envoyer ».

Remarque : il n'est pas nécessaire de renseigner dans ce carnet d'adresses les IPS-Firewalls sur lesquels l'envoi des traces par le NETASQ Syslog est activé. En effet, lorsque le NETASQ Log Collector se connecte à un IPS-Firewall, il vérifie si cette option est activée ou non avant de télécharger les traces. Si l'option est activée, le NETASQ Log Collector ne télécharge pas les traces en local mais directement dans le répertoire du Syslog. Les paramètres de connexion ne doivent donc pas être renseignés dans le carnet d'adresses.

Base de données



Il est possible d'utiliser une base de type MySql ou une base de type Interbase. Il est obligatoire de renseigner le type de base de données utilisé. Il est fortement recommandé d'utiliser MySQL. Deux indicateurs rendent compte de la taille de la base de données et de l'espace disque restant.

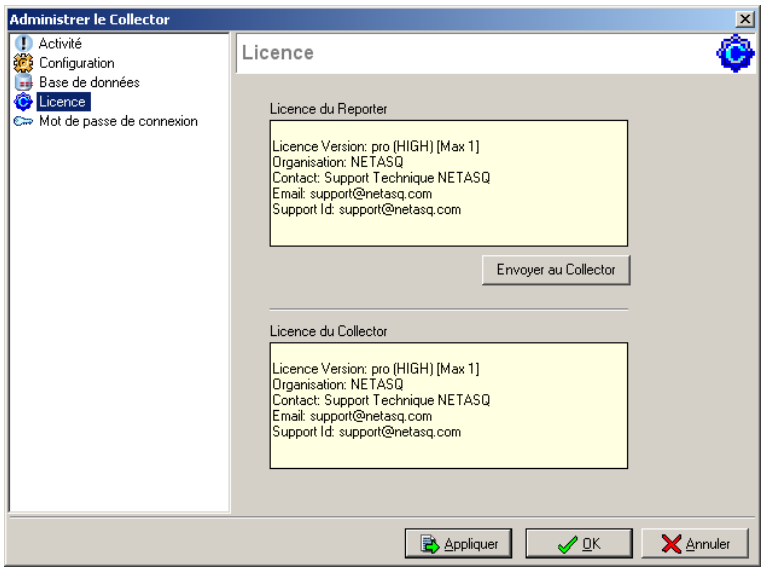
Changement des mots de passe de la base de données

Les deux boutons de ce menu vous permettent de modifier les mots de passe des comptes root et reporter de la base de données.

Comme indiqué dans l'écran, il est nécessaire d'arrêter le Collector pour procéder aux modification précédentes. De plus les mots de passe sont transmis en clair sur le réseau.

Il est très fortement recommandé de modifier les mots de passe à la première utilisation du Reporter PRO. Les mots de passe par défaut sont : netasq pour le compte reporter et v7ZVIMFvWuTHeaA8 pour le compte root.

Licence



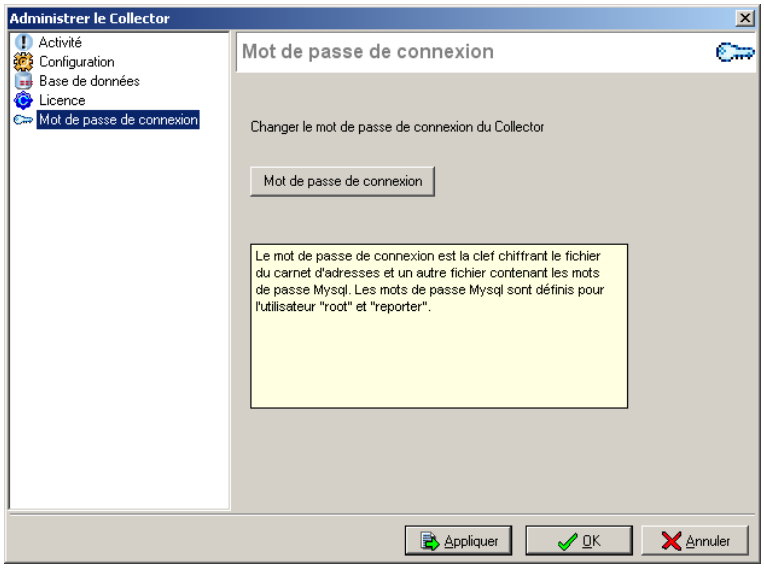
Ce menu vous permet d'insérer une nouvelle licence dans votre Collector. Cette licence vous est indispensable pour activer les options que vous désirez (nombre de firewalls, type de firewall,…).

Si vous aviez auparavant installé un Log Analyzer, cette licence est réutilisée dans la suite d'administration PRO (vous pouvez copier le fichier « licence » du répertoire d'installation du Log Analyzer dans le répertoire d'installation du Reporter PRO). Sinon la suite d'administration PRO est livrée avec une licence d'exploitation d'un seul firewall nommée « licence HIGH ».

Pour pouvoir gérer les traces de plusieurs IPS-Firewalls à la fois et garantir une meilleure administration des flux transitant par vos IPS-Firewalls, vous devez obtenir une licence illimitée.

© Copyright NETASQ 2006

Mots de passe de connexion


Administrer le Collector
Activité
Configuration
Base de données
Licence
Mot de passe de connexion
Mot de passe de connexion
Changer le mot de passe de connexion du Collector
Mot de passe de connexion
Le mot de passe de connexion est la clef chiffrant le fichier du carnet d'adresses et un autre fichier contenant les mots de passe Mysql. Les mots de passe Mysql sont définis pour l'utilisateur "root" et "reporter".
Appliquer
OK
Annuler

Ce menu n'est utilisé que pour modifier le mot de passe principal, celui-ci qui est utilisé pour la connexion au NETASQ Log Collector ainsi que pour le chiffrement des mots de passe de la base de données.

Si vous aviez auparavant installé un Log Analyzer, le mot de passe principal correspond à celui de l'ancien carnet d'adresses. Sinon le mot de passe par défaut est « netasq ».

Il est très fortement recommandé de modifier ce mot de passe à la première utilisation du Reporter PRO.

© Copyright NETASQ 2006

Activité du Log Collector

Le NETASQ Log Collector effectue la collecte des traces de façon séquentielle : il se connecte à tour de rôle à chaque IPS-Firewall. Entre chaque rotation complète (connexion à tous les IPS-Firewalls), le NETASQ Log Collector se met en veille. Le temps de veille dépend de l'activité de l'IPS-Firewall (donc du nombre de lignes de traces générées), plus l'activité de l'IPS-Firewall est importante plus le temps de veille du NETASQ Log Collector sera faible. Le temps de veille peut varier de 5 secondes à 30 minutes.

© Copyright NETASQ 2006

Section D

NETASQ AutoReport (Version PRO)

© Copyright NETASQ 2006

Les traces générées par les IPS-Firewalls relatent les événements survenus sur votre réseau. Elles exposent les comportements des trafics surveillés et les tentatives d'intrusion de votre réseau. Utilisées pour adapter la politique de sécurité aux menaces en perpétuelle évolution, elles constituent des informations sensibles assurant un historique exhaustif des trafics transitant par votre IPS-Firewall.

L'exploitation de ces traces peut s'avérer parfois fastidieux et rébarbatif si les outils utilisés ne sont pas adaptés. Souvent volumineux (du fait de leur exhaustivité), les fichiers de traces possèdent très souvent les clefs pour l'identification de problèmes sur le réseau. Pourtant, bien souvent perdus dans la somme des informations, ces problèmes passent inaperçus si les outils utilisés ne sont pas adaptés. NETASQ possèdent une gamme d'outils (Reporter version standard et PRO, Log Collector, Syslog…) de gestion des traces qui aident les administrateurs dans l'extraction des informations recherchées pour une meilleure réactivité et un meilleur résultat.

Le générateur automatique de rapport « Autoreport » NETASQ est un nouvel outil mis à la disposition des administrateurs pour la gestion de leurs traces. Modulable et complètement personnalisable, « l'Autoreport » de NETASQ exploite la richesse des traces remontées par les IPS-Firewalls NETASQ. Mise en forme dans un rapport HTML divisé en sections (contenant chacune : un titre, un intitulé, un tableau et un graphique), l'information est structurée. Les faiblesses ou incohérences du système apparaissent alors rapidement et les mesures adéquates peuvent être envisagées avec promptitude.

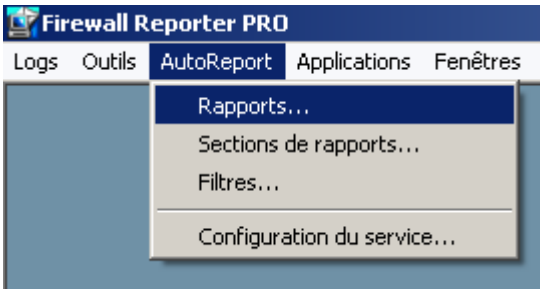
Autoreport de NETASQ est un outil unique de génération de rapports. En effet grâce à cet outil vous pouvez analyser l'information que vous choisissez et uniquement cette information. Pour cela vous créez les sections du rapport (ou vous utilisez les modèles déjà définis par NETASQ) selon vos besoins propres. Le rapport présente alors dans un format HTML facilement consultable, les résultats de votre requête sous la forme d'un tableau et d'un graphique. Un tableau pour une visualisation rapide et juste des indicateurs que vous avez défini, un graphique pour une visualisation d'ensemble vous permettant de déduire des tendances sur les différents facteurs surveillés.

Reporter PRO

Autoreport est associé au NETASQ Reporter PRO pour fonctionner. En effet l'Autoreport utilise la base de données du NETASQ Collector contenu dans le package du NETASQ Reporter PRO pour récupérer les traces nécessaires à la génération des rapports.

© Copyright NETASQ 2006

La configuration de l'autoreport est réalisée dans l'interface de configuration du Reporter PRO puisque l'autoreport est désormais une partie intégrante du Reporter PRO.



La configuration de l'autoreport se compose des menus de configuration suivants :

► **Rapports** : date et intervalle de génération des rapports, IPS-Firewalls concernés, sections du rapport et commentaires associés au rapport ;

► **Section de rapports** : contenu de la section, présentation des informations et commentaires associés à la section ;

► **Filtres :** définition des filtres SQL, type de traces par type de traces. Exemples : sélection des alarmes mineures uniquement, sélection des alarmes majeures, traces provenant de l'adresse IP x.x.x.x ;

► **Configurer le service** : paramètres de la base de données et emplacement du rapport généré.

© Copyright NETASQ 2006

La première étape de l'utilisation de l'outil NETASQ Autoreport est la mise en place du service et son démarrage. Afin de faciliter l'utilisation d'autoreport le package d'installation NETASQ installe et démarre le service en même temps qu'il installe le reste des logiciels sélectionnés lors de l'installation.

Ainsi à la fin de l'installation de l'autoreport, le service est déjà démarré. Vous avez tout de même la possibilité d'installer/désinstaller et de démarrer/arrêter le service.

Procédure d'installation du service

Le service « Autoreport Log Reporter » est installé automatiquement à l'installation. Il est cependant possible de l'installer en lançant un exécutable « **Installer – Lancer le service Autoreport** » se trouvant dans le menu :

`Démarrer>Programmes>NETASQ>Administration Suite x.x>Services`

Sinon, la procédure complète est la suivante :

1. Ouvrez une invite de commandes DOS,
2. Placez-vous sur le répertoire NETASQ de votre disque dur (c:\Program Files\NETASQ\Administration Suite <version> par défaut),
3. Tapez la commande d'installation suivante : servautoreport.exe /INSTALL /SILENT,
4. Tapez la commande de démarrage du service : NET START servautoreport.

Une fois installé, le service sera redémarré à chaque reboot même si aucune session n'est ouverte.

Procédure de désinstallation du service

Le service Autoreport Log Reporter peut être désinstallé à l'aide de l'exécutable « **Arrêter – Retirer le service Autoreport** » se trouvant dans le menu :

`Démarrer>Programmes>NETASQ>Administration Suite x.x>Services`

Sinon, la procédure complète est la suivante :

1. Ouvrez une invite de commandes DOS,
2. Tapez la commande d'arrêt du service suivante : NET STOP servautoreport,
3. Placez-vous dans le répertoire NETASQ de votre disque dur (c:\Program Files\NETASQ\Administration Suite <version> par défaut),
4. Tapez la commande de désinstallation du service : servautoreport.exe /UNINSTALL /SILENT.

Il est recommandé d'arrêter et de redémarrer le service MySQL à l'aide de l'outil de gestion des services inclus avec Windows NT, 2000 et XP.

© Copyright NETASQ 2006

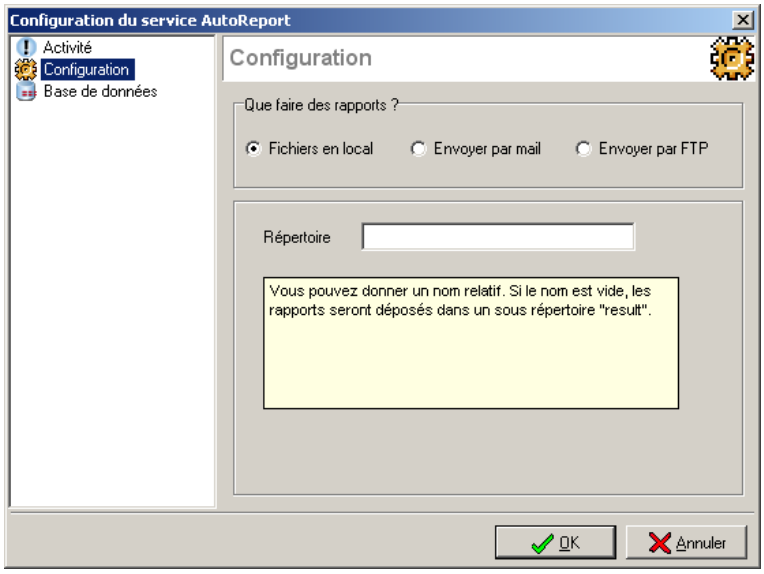
Configurer le service

Activité du service

La zone d'activité du service présente les messages remontés par le service lors de son exécution. Le tableau ci-dessous regroupe ces messages et apporte une explication succincte de chacun d'eux.

Loaded (x reports)	Au démarrage du service celui effectue une découverte des rapports actuellement configurés.
List all reports	Ce message indique que les informations relatives à chacun des rapports découverts vont être affichées.
Report N°…	Sous la forme d'une phrase, le service indique le numéro, le nom, l'intervalle de génération et la date de dernière génération de chacun des rapports découverts.
Execute report	Ce message indique qu'un rapport est en cours de réalisation.
Last executed	Date de dernière génération du rapport en train d'être réalisé.
From…to…	Intervalle de temps concerné par le rapport en train d'être réalisé.
Execution ok	L'exécution du rapport s'est déroulée avec succès.
Execution NOT ok	L'exécution du rapport a échouée.
Reloaded	Toutes les 30 secondes, le service effectue une redécouverte des rapports actuellement configurés.
Service Launched	Le service est lancé.
Service Stopped	Le service est stoppé.
Les erreurs FTP	Etant donné qu'il est possible de déposer les rapports nouvellement créés sur un serveur FTP. Le service renvoie les erreurs qu'il reçoit de la part du serveur FTP.

Configuration



L'outil Autoreport vous permet de définir l'emplacement de destination des rapports générés. Trois possibilités sont offertes par NETASQ :

Fichier en local	Vous devez spécifier le chemin complet du répertoire de destination.
Envoyé par mail	Vous devez spécifier le serveur SMTP d'expédition (Adresse IP ou nom de machine), votre accompte sur ce serveur SMTP (sous la forme d'une adresse e-mail) et l'adresse e-mail de destination.
Envoyé par FTP	Vous devez spécifier le serveur FTP (Adresse IP ou nom de machine), votre login et mot de passe sur ce serveur FTP, le répertoire de destination sur ce serveur FTP.

Dans le cas de l'envoi par mail et par FTP, vous pouvez tester les informations que vous avez indiquées en cliquant sur le bouton « **Tester** » du menu.

Base de données

L'Autoreport utilise une base de données MySQL du type du Collector pour générer les rapports HTML. Ainsi pour permettre la génération des rapports vous devez spécifier les informations d'accès à une base de données. Deux paramètres sont nécessaires pour cet accès : l'adresse IP de l'hôte sur lequel se situe la base de données et le mot de passe de la base de données (Rappel : par défaut le mot de passe de la base de données du Log Collector contenu dans le NETASQ Reporter PRO est « **reporter** »

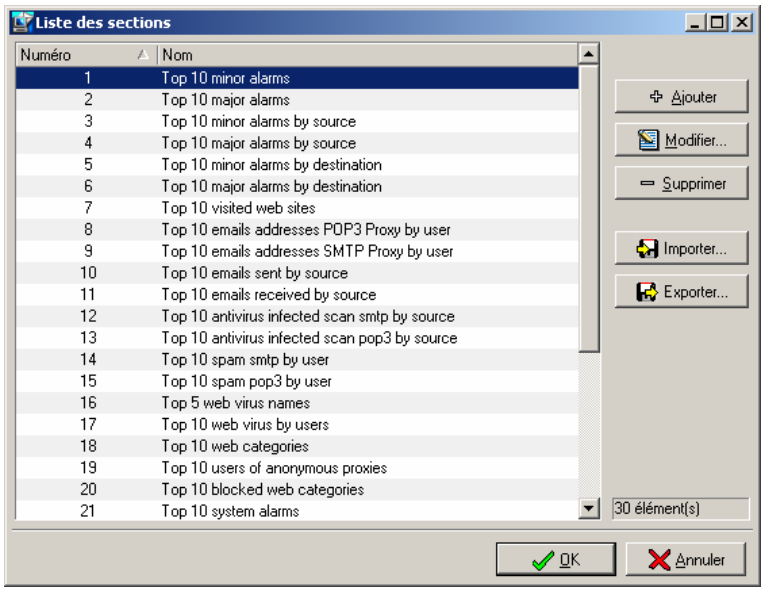
En spécifiant l'adresse IP « **127.0.0.1** », l'outil Autoreport recherchera une base de données située sur la machine où il est exécuté.

La construction des rapports est effectuée en deux étapes : la définition des sections de rapports et ensuite l'affectation des sections au sein d'un rapport.

Sections de rapports

Liste des sections

Lorsque vous cliquez sur « **Sections de rapports** » dans le menu « **Autoreport** » la fenêtre suivante apparaît :

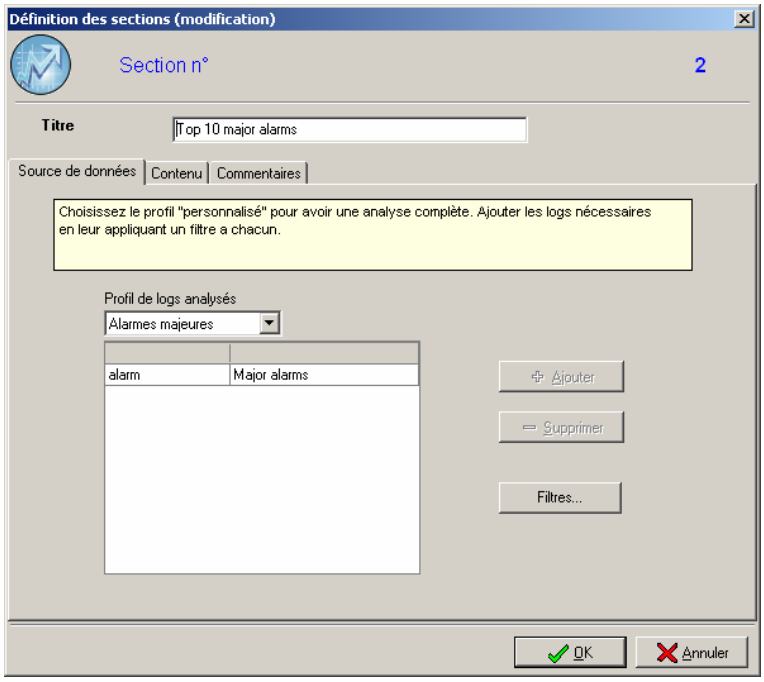

Liste des sections
Numéro
Nom
1 Top 10 minor alarms
2 Top 10 major alarms
3 Top 10 minor alarms by source
4 Top 10 major alarms by source
5 Top 10 minor alarms by destination
6 Top 10 major alarms by destination
7 Top 10 visited web sites
8 Top 10 emails addresses POP3 Proxy by user
9 Top 10 emails addresses SMTP Proxy by user
10 Top 10 emails sent by source
11 Top 10 emails received by source
12 Top 10 antivirus infected scan smtp by source
13 Top 10 antivirus infected scan pop3 by source
14 Top 10 spam smtp by user
15 Top 10 spam pop3 by user
16 Top 5 web virus names
17 Top 10 web virus by users
18 Top 10 web categories
19 Top 10 users of anonymous proxies
20 Top 10 blocked web categories
21 Top 10 system alarms
Ajouter
Modifier...
Supprimer
Importer...
Exporter...
30 élément(s)
OK
Annuler

Les boutons d'actions situés sur la droite de la fenêtre vous permettent d'ajouter, de modifier ou de supprimer une section.

Définition des sections

Si vous cliquez sur le bouton « Ajouter » ou « Modifier » de l'écran présentant la liste des sections présentes, la fenêtre suivante apparaît :

© Copyright NETASQ 2006



Le titre de la fenêtre vous indique si vous êtes dans une phase de création d'une section ou dans une phase de modification d'une section.

Pour identifier votre section, spécifiez un titre pour celle-ci. De plus chaque section se définit grâce à trois onglets : « Source de données », « Contenu » et « Commentaires ».

Source de données

Choisissez parmi les profils de logs configurés (alarmes mineures, alarmes majeures, web, mails,ftp) ou définissez votre propre profil en sélectionnant « Personnalisé ».

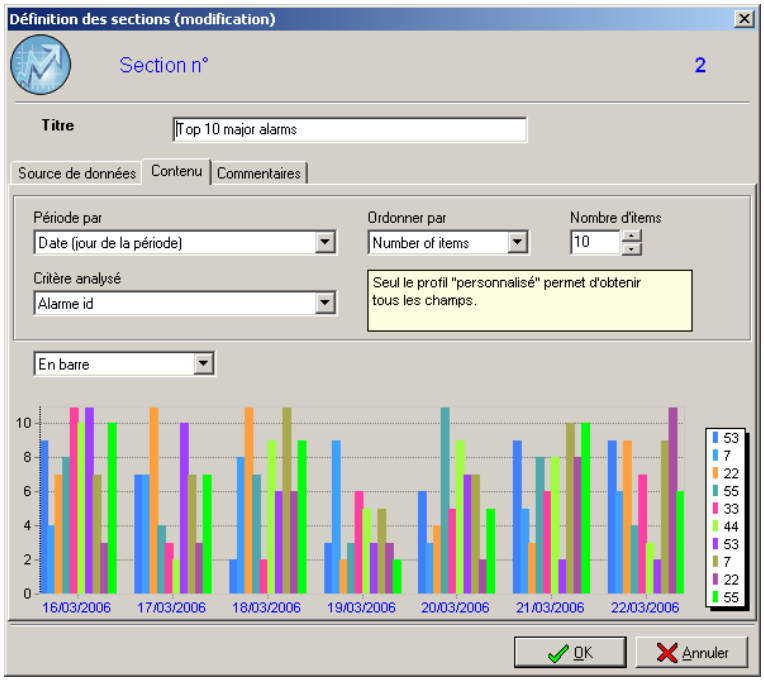
Sous le profil de logs, apparaît alors les protocoles et les filtres qui seront pris en compte. Par exemple : si vous sélectionnez le profil de logs « Alarmes majeures », vous verrez apparaître le filtre « alarm : major alarms ».

Pour définir un profil personnalisé, sélectionnez d'abord un type de logs parmi : web, alarm, connection, filter, smtp, plugin, pop3, puis choisissez les filtres SQL associés. Ajouter les différents filtres en cliquant sur Ajouter. Attention les profils de logs configurés par défaut ne peuvent être modifiés.

Pour définir vos propres filtres SQL, cliquez sur le bouton « Filtres » et reportez-vous à la section « Constructeur de filtres » de ce document pour plus d'informations sur la construction des filtres SQL.

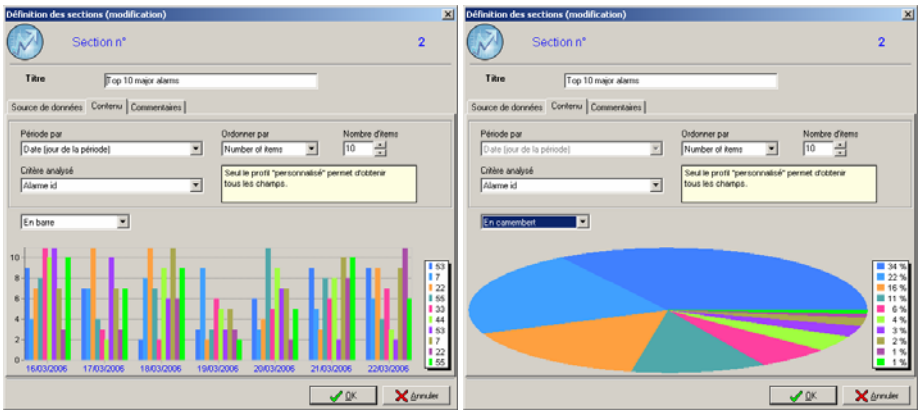
© Copyright NETASQ 2006

Contenu



Période par	Cette option permet de définir de quelle façon est présentée l'échelle horizontale des données parmi : chaque jour de la période, par jour de la semaine ou selon un créneau horaire.
Critère analysé	Définissez les regroupements qui doivent être effectués parmi : adresses sources, adresses destination, protocole ou utilisateurs.
Ordonné par	(ne s'applique pas aux alarmes) Tri des données par nombre d'items volume du trafic, volume envoyé ou volume reçu.
Nombre d'items	Nombre de regroupements affichés. Cela permet de réaliser des rapports du type « les 5 plus gros… » ou « les 10 plus gros… ».

De plus chaque graphique peut être affiché sous la forme de barre ou de camembert.



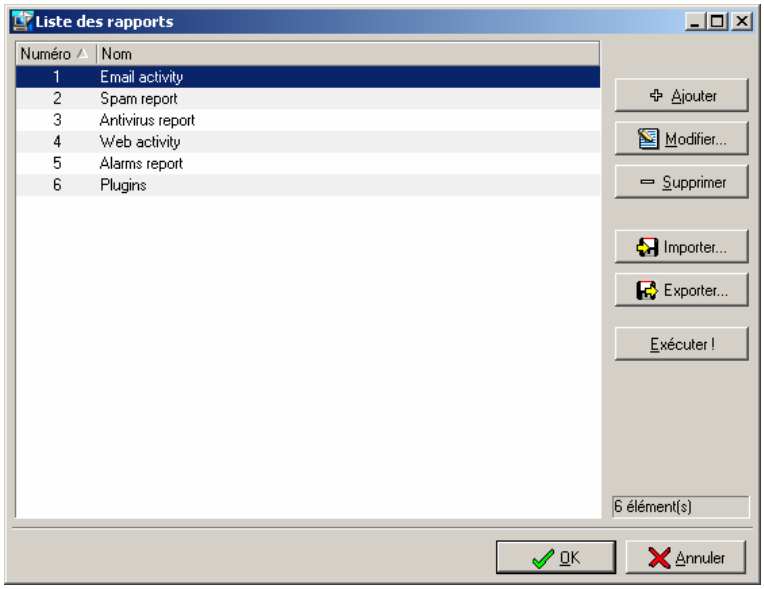
Commentaires

Dans cette zone de commentaire, vous spécifiez un texte explicatif de la section qui va être affichée. Ainsi vous pouvez personnaliser totalement vos rapports.

Rapports

Liste des rapports

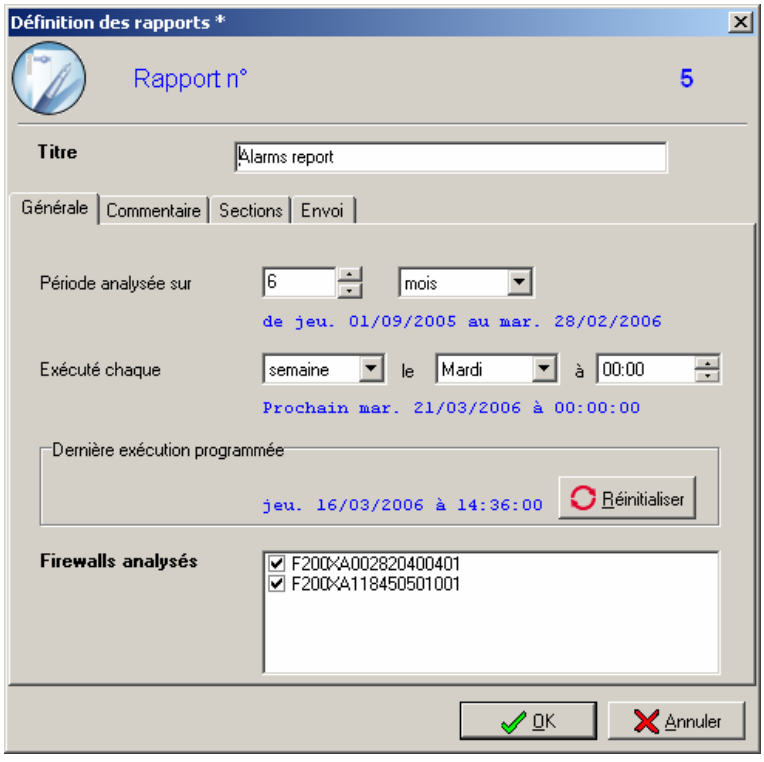
Lorsque vous cliquez sur « **Rapports** » dans le menu « **Autoreport** » la fenêtre suivante apparaît :



Les boutons d'actions situés sur la droite de la fenêtre vous permettent d'ajouter, de modifier ou de supprimer un rapport.

Définition des rapports

Si vous cliquez sur le bouton « Ajouter » ou « Modifier » de l'écran présentant la liste des rapports présents, la fenêtre suivante apparaît :



Pour identifier votre rapport, spécifiez un titre pour celui-ci. De plus chaque rapport se définit grâce à trois onglets : « Générale », « Commentaire » et « Sections ».

Générale

Période analysée	Cette option permet de spécifier la période analysée en choisissant l'intervalle de temps concerné.
Exécuté chaque	Cette option permet de définir le jour de génération du rapport soit jour par jour soit un jour dans la semaine soit un jour dans le mois. La zone dynamique située sous l'option « Exécuté chaque jour » synthétise la configuration. La date de dernière exécution peut être initialisée grâce au bouton du même nom.
Firewalls analysés	La liste des IPS-Firewalls concernés par le rapport est tirée de la base de données. Tant que l'outil « Autoreport » ne peut se connecter à la base, cette liste n'apparaît pas.

Commentaire

Dans cette zone de commentaire, vous spécifiez un texte explicatif du rapport qui va être affiché. Ainsi vous pouvez personnaliser totalement vos rapports.

Sections

Le dernier onglet permet de définir les sections présentées dans le rapport parmi les sections définies précédemment.

Envoi

Bien qu'il soit possible de définir de manière globale, où et comment seront enregistrés les rapports HTML générés, rapport par rapport, il est possible de définir une méthode différente de la méthode globale.

Configuration globale	Si vous spécifiez cette méthode d'envoi, le rapport HTML sera généré et stocké selon la méthode que vous aurez défini dans la configuration du services.
Fichiers locaux	Vous devez spécifier le chemin complet du répertoire de destination.
Envoyé par mail	Vous devez spécifier le serveur SMTP d'expédition (Adresse IP ou nom de machine), votre accompte sur ce serveur SMTP (sous la forme d'une adresse e-mail) et l'adresse e-mail de destination.
Envoyé par FTP	Vous devez spécifier le serveur FTP (Adresse IP ou nom de machine), votre login et mot de passe sur ce serveur FTP, le répertoire de destination sur ce serveur FTP.

Dans le cas de l'envoi par mail et par FTP, vous pouvez tester les informations que vous avez indiquées en cliquant sur le bouton « **Tester** » du menu.

© Copyright NETASQ 2006

Chapitre XV

Annexes

© Copyright NETASQ 2006

Annexe A : Contrôle des saisies

Durant la configuration du Firewall, vous êtes amené à saisir au clavier différents types de données :

- ► Adresse IP,
- ► Commentaires,
- ► Nom de fichier,
- ► Nom d'objets (machine, réseau, service),

Chacun de ces types de données accepte un ensemble précis de caractères, ces caractères sont filtrés durant la saisie du paramètre.

Adresse IP

Les chiffres de « 0 » à « 9 » et le « . » sont les seuls caractères gérés. Pour effacer un caractère, vous pouvez utiliser la touche « Backspace » ou « Suppr ».

Commentaires

Vous pouvez utiliser les moyens classiques de mouvement du curseur durant l'édition d'un commentaire (souris, flèches au clavier).

Nom de fichier

Vous pouvez utiliser les moyens classiques de mouvement du curseur durant l'édition d'un commentaire (souris, flèches au clavier).

Nom d'objets

Certains caractères comme les accents et les espaces ne sont pas gérés dans les noms d'objets. Durant l'édition d'un nom d'objet, quand un caractère accentué est saisi au clavier, le logiciel de configuration insère le caractère non accentué correspondant. Un caractère non géré n'est pas validé et n'apparaît pas à l'écran.

Vous pouvez utiliser les moyens classiques de mouvement du curseur durant l'édition d'un commentaire (souris, flèches au clavier).

© Copyright NETASQ 2006

Annexe B : Services TCP/IP

Dans cette annexe vous trouverez la liste de services TCP et UDP couramment utilisés tels que : FTP, Telnet, www, SMTP,...

Cette annexe vous est présentée sous la forme d'une liste composée de quatre colonnes :

- ► Une colonne contenant le nom du service,
- ► Une colonne contenant le numéro de port associé au service,
- ► Une colonne indiquant le protocole utilisé (TCP et/ou UDP),
- ► Une colonne contenant une description du service.

Nous vous conseillons de ne pas saisir tous ces services lorsque vous définissez la liste des objets, afin de ne pas surcharger votre affichage et de gagner en visibilité.

Service	Port	Protocole	Description
echo	7	TCP/UDP	Echo
discard	9	TCP	Discard
systat	11	TCP/UDP	Systat
daytime	13	TCP/UDP	Daytime
qotd	17	TCP/UDP	Quote of The Day
chargen	19	TCP/UDP	Character generator
ftp-data	20	TCP	File Transfer (Default Data)
ftp	21	TCP	File Transfer (Control)
telnet	23	TCP	Telnet
smtp	25	TCP	Simple Mail Transfer
time	37	TCP/UDP	
rip	39	UDP	Ressoure Locator Protocol
nameserver	42	TCP/UDP	Host Name Server
nicname	43	TCP	
login	49	TCP/UDP	
domain	53	TCP/UDP	Domain Name Server (DNS)
sql-net	66	TCP/UDP	Oracle SQL Net
bootps	67	UDP	Bootstrap Protocol Server
bootpc	68	UDP	Bootstrap Protocol Client
tftp	69	TCP/UDP	Trivial File Transfer
gopher	70	TCP	Gopher
finger	79	TCP	Finger
www	80	TCP	World Wide Web
kerberos	88	TCP/UDP	Kerberos
npp	92	TCP/UDP	Network Printing Protocol
hostname	101	TCP	NIC Host Name Server
iso-tsap	102	TCP	ISO-TSAP Class 0
rtelnet	107	TCP	Remote Telnet Service
pop2	109	TCP	Post Office Protocol version 2
pop3	110	TCP	Post Office Protocol version 3
sunrpc	111	TCP / UDP	SUN Remote Procedure Call
auth	113	TCP	Authentication Service
uucp-path	117	TCP	
sqlserv	118	TCP / UDP	SQL Services
nntp	119	TCP	Network News Transfer Protocol
ntp	123	UDP	Network Time Protocol
epmap	135	TCP / UDP	Netbios Net Service

© Copyright NETASQ 2006

Service	Port	Protocole	Description
netbios-ns	137	TCP / UDP	DCE endpoint resolution
netbios-dgm	138	UDP	Netbios Datagram Service
netbios-ssn	139	TCP	Netbios session service
imap2	143	TCP	Interim Mail Access Protocol version 2
sql-net	150	TCP / UDP	SQL-NET
snmp	161	UDP	Simple Network Management Protocol
snmptrap	162	UDP	SNMP trap
print-srv	170	TCP	
bgp	179	TCP	Border Gateway Protocol
irc	194	TCP	Internet Relay Chat Protocol
ipx	213	UDP	IPX over IP
imap3	220	TCP / UDP	Internet Message Access Protocol 3
ldap	389	TCP	Lightweight Directory Access Protocol
netware-ip	396	TCP / UDP	Novell Netware over IP
ups	401	TCP / UDP	Uninterruptible Power Supply
smpte	420	TCP / UDP	SMPTE
https	443	TCP / UDP	Https Mcom
microsoft-ds	445	TCP / UDP	
kpasswd	464	TCP / UDP	Kerberos (v5)
isakmp	500	UDP	Internet Key Exchange
exec	512	TCP / UDP	Remote process execution
biff	512	TCP / UDP	Notify user of new mail received
login	513	TCP / UDP	Remote login
who	513	TCP / UDP	Who's logged in to machines
cmd	514	TCP / UDP	Remote exec
syslog	514	TCP / UDP	
printer	515	TCP	Spooler
talk	517	UDP	
ntalk	518	UDP	
router	520	TCP / UDP	Extended File Name Server
timed	525	UDP	Timeserver
tempo	526	TCP	
courier	530	TCP	
conference	531	TCP	
uucp	540	TCP	
klogin	543	TCP	Kerberos login
kshell	544	TCP	Kerberos remote shell
remotefs	556	TCP	Remote login using Kerberos
rmonitor	560	UDP	
rmonitor	561	UDP	
whoami	565	TCP / UDP	
ldaps	636	UDP	LDAP over TLS/SSL
kerberos-adm	749	TCP / UDP	Kerberos administration
kerberos-iv	750	UDP	Kerberos version IV

Type	Code	Description	Requête	Erreur
0	0	echo reply	x	
3		Destination unreachable :		
	0	network unreachable		x
	1	host unreachable		x
	2	protocol unreachable		x
	3	port unreachable		x
	4	fragmentation needed but don't fragment bit set		x
	5	source route failed		x
	6	destination network unknown		x
	7	destination host unknown		x
	8	source host isolated (obsolete)		x
	9	destination network administratively prohibited		x
	10	destination host administratively prohibited		x
	11	network unreachable for TOS		x
	12	host unreachable for TOS		x
	13	communication administratively prohibited by filtering		x
	14	host precedence violation		x
	15	precedence cutoff in effect		x
4	0	source quench	x	
5		redirect :		
	0	redirect for network		x
	1	redirect for host		x
	2	redirect for type of service and network		x
	3	redirect for type of service and host		x
8	0	echo request	x	
9	0	routeur advertisement		
10	0	routeur solicitation		x
11		time exceedeed :		x
	0	time to live equals 0 during transit		
	1	time to live equals 0 during reassembly		x
12		parameter problem :		
	0	IP header bad		x
	1	required option missing		x
13	0	timestamp request	x	
14	0	timestamp reply	x	
15	0	information request (obsolete)	x	
16	0	information reply (obsolete)	x	
17	0	address mask request	x	
18	0	address mask reply	x	

© Copyright NETASQ 2006

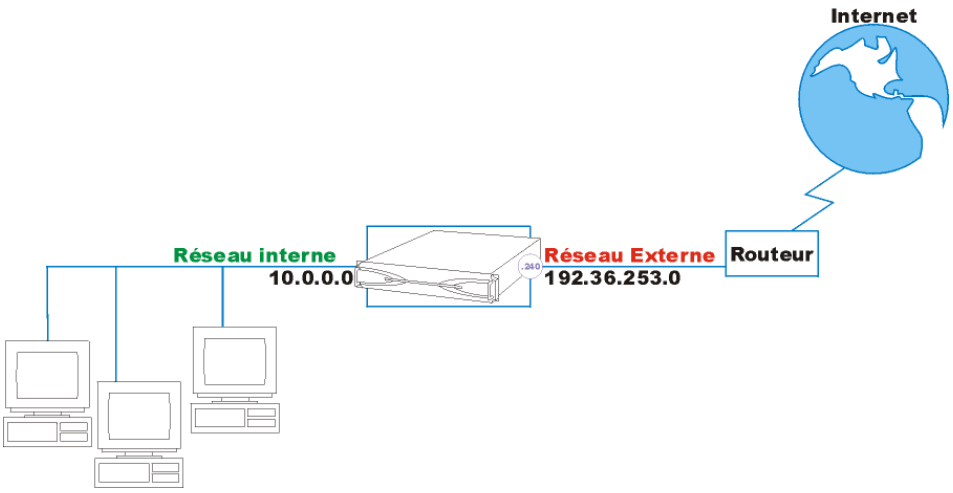
Annexe D : Exemples de translations d'adresses

Les exemples ci-dessous illustrent différentes configurations utilisant la translation d'adresse. Ils utilisent les différentes possibilités offertes suivants les besoins et l'architecture réseau, dans des cas volontairement simplifiés.

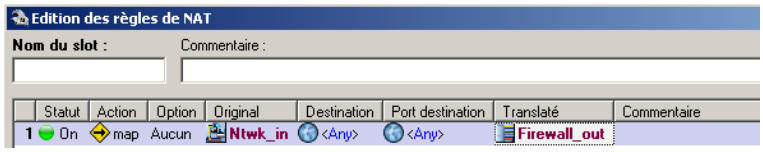
► Translation unidirectionnelle du réseau interne pour accès à l'Internet,
► Configuration avec un serveur Web dans la DMZ,
► Configuration avec un serveur web dans la DMZ qui doit être accessible du réseau interne et externe avec son adresse officielle,
► Connexion par modem sur le port série du firewall de l'accès Internet,
► Redirection de port : utilisation d'une seule adresse IP pour contacter plusieurs serveurs,
► Partage de charge : distribution des connexions sur un pool de serveurs.

Exemple 1 : translation unidirectionnelle d'une classe d'adresses

L'exemple ci-dessous donne un exemple de configuration de translation d'adresses unidirectionnelle de l'ensemble du réseau interne vers une adresse virtuelle sur le réseau externe.



Au niveau du Firewall, la configuration de la translation d'adresses correspondante est :



Typiquement, cette configuration permet à l'ensemble des postes se situant sur le réseau interne d'accéder à Internet.

Les machines sortent du réseau avec l'adresse virtuelle 192.36.253.240 et peuvent recevoir les réponses à leurs requêtes.

Il faut bien entendu que l'adresse virtuelle sur le réseau externe soit routable sur Internet (adresse officielle).

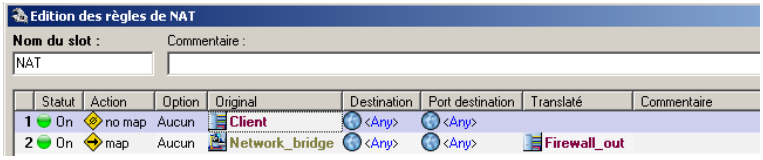
© Copyright NETASQ 2006

Cependant, les machines internes ne sont pas joignables de l'extérieur (unidirectionnelle); si une demande de connexion vers l'adresse 192.36.253.240 arrive au firewall, aucune translation d'adresses n'est effectuée vers une adresse d'une machine du réseau interne.

En passant en configuration avancée (bouton « »), on remarque que cette règle translate les ports destination sur une plage appelée ephemeral_fw (port 20000 à 59999). Cela signifie que non seulement l'adresse source est translatée mais aussi le port source. Le firewall utilise un port disponible pour la translation dans cette plage, ce qui évite les conflits si deux machines du réseau interne utilisent le même port source.

Si vous désirez retirer une machine de l'opération de map (l'adresse IP de cette machine ne sera pas translatée), utilisez l'opération "no map".

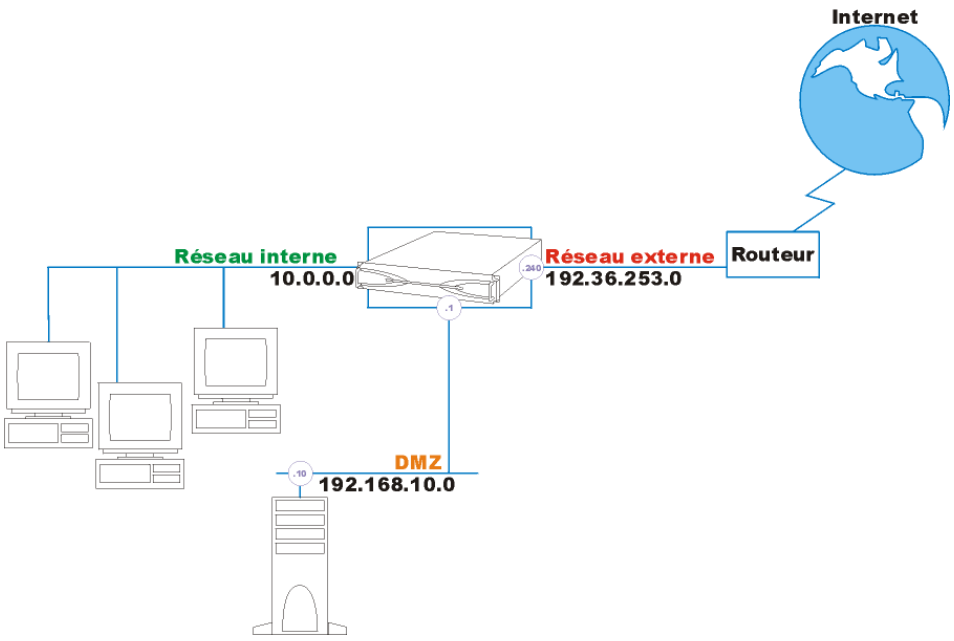
L'exemple suivant montre comment retirer une machine de l'opération de map (les adresses IP spécifiées ne correspondent plus à l'exemple précédent) :



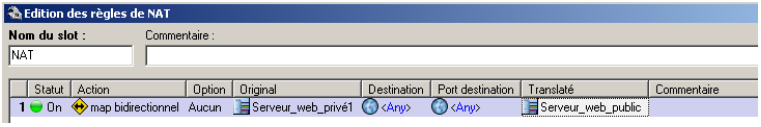
Ici la machine "Client" ne sera pas mappée.

Exemple 2 : translation bidirectionnelle

L'exemple ci-dessous illustre une configuration dans laquelle figure un serveur Web dans la DMZ.



La configuration de la translation d'adresses sur le Firewall doit être la suivante :

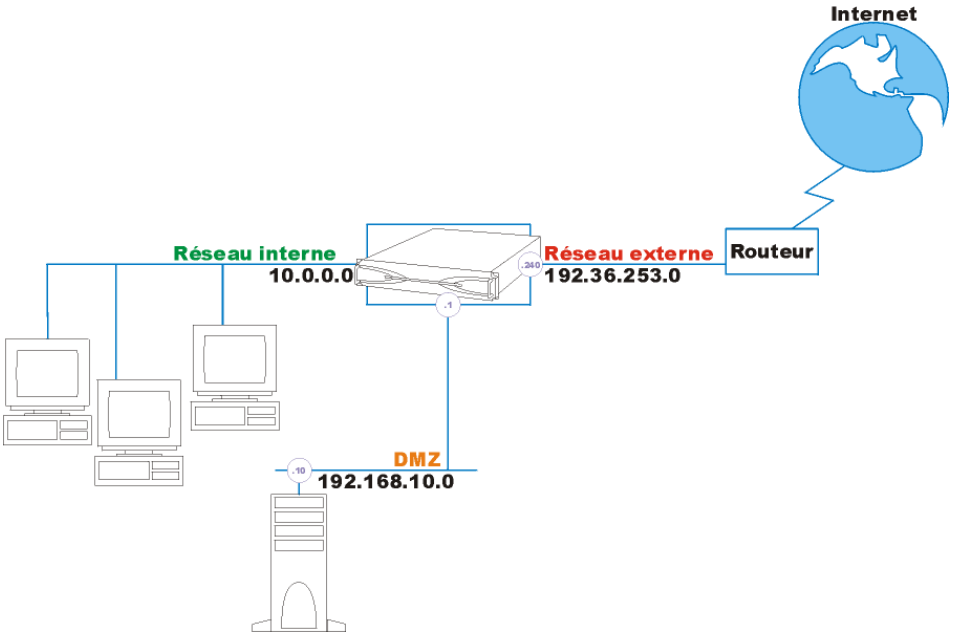


Avec la translation d'adresses bidirectionnelle, le serveur est accessible de l'extérieur. L'adresse utilisée à l'extérieur est l'adresse virtuelle, routable sur l'Internet.

Ainsi les requêtes provenant de l'extérieur (direction OUT) avec adresse de destination 192.36.253.10 sont changées en 192.168.10.10 et routées par le Firewall vers la DMZ.

Exemple 3 : Accès à un serveur WEB en DMZ

L'exemple ci-dessous illustre une configuration avec trois sous-réseaux (interne, externe et DMZ) et un serveur web dans la DMZ. On veut que le serveur web soit accessible de l'extérieur mais aussi à partir du réseau interne, avec son adresse officielle (virtuelle).

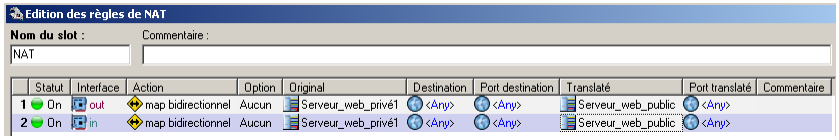


Si un poste sur le réseau interne veut se connecter au serveur web via son URL, la première chose effectuée est la résolution DNS.

Dans le cas où le serveur DNS est externe, il va renvoyer l'adresse virtuelle du serveur web connu sur Internet (192.36.253.10). La machine envoie donc sa requête avec cette adresse en destination. La machine visée n'existant pas sur le réseau externe, la requête est envoyée sur l'Internet et se perd ou renvoie une erreur. Elle peut aussi être renvoyée par le routeur.

Il faut donc translater sur l'interface interne du Firewall cette adresse virtuelle en l'adresse réelle du serveur dans la DMZ. On veut aussi que le serveur soit accessible depuis le réseau externe avec cette adresse virtuelle.

On a donc deux fois la même règle mais qui s'appliquent sur des interfaces différentes. Le choix de l'interface se fait en mode avancé (bouton « Mode Avancé »). Par défaut, le firewall choisit l'interface où se trouve l'adresse IP virtuelle (OUT dans l'exemple).


Edition des règles de NAT
Nom du slot :
NAT
Commentaire :
Statut Interface Action Option Original Destination Port destination Translaté Port translaté Commentaire
1 On out map bidirectionnel Aucun Serveur_web_privé1 <Any> <Any> Serveur_web_public <Any>
2 On in map bidirectionnel Aucun Serveur_web_privé1 <Any> <Any> Serveur_web_public <Any>

Ainsi les requêtes provenant de l'extérieur (Interface OUT) et du réseau interne (Interface IN) avec l'adresse de destination 192.36.253.10 sont changées en 192.168.10.10 et routées directement par le Firewall vers la DMZ.

Remarques

L'ordre des règles est ici important. Il faut pour ce cas mettre en premier lieu la règle avec l'adresse IP virtuelle et l'interface réseau (direction) appartenant au même réseau. Dans notre exemple, l'adresse virtuelle appartient au réseau externe (OUT). Il faut donc mettre la règle avec comme direction l'interface OUT en premier.

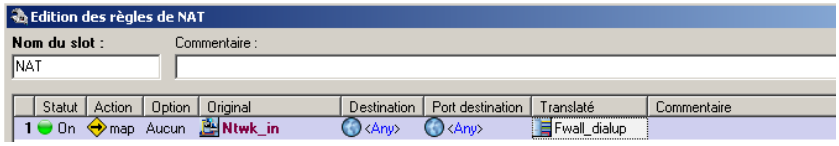
Il n'est pas possible de contacter le serveur avec son adresse virtuelle si le client et le serveur sont réellement sur le même réseau. En effet, le message arrivera bien au serveur mais celui-ci va répondre directement au client (car ils sont sur le même réseau) avec son adresse réelle. Le client reçoit alors la réponse avec une adresse différente de sa requête initiale et rejette le paquet.

Exemple 4 : connexion Internet par modem

Dans le cas d'une connexion modem, sur le port série ou l'interface externe du firewall NETASQ, il faut translater les adresses des machines internes voulant utiliser le modem.

On doit translater les adresses vers l'adresse firewall_dialup. Cette interface possède l'adresse IP (fixe ou non) négociée avec le provider lors de la demande de connexion.

Dans cet exemple, on veut donner accès au réseau interne à Internet via le modem installé sur le port série du boîtier :


Edition des règles de NAT
Nom du slot :
NAT
Commentaire :
Statut Action Option Original Destination Port destination Translaté Commentaire
1 On map Aucun Ntwk_in <Any> <Any> Fwall_dialup

Si vous fonctionnez en mode transparent vous devez mettre cette règle en place (en remplaçant l'objet *Network_in* par *Network ou Bridge*) pour pouvoir accéder à Internet avec votre modem.

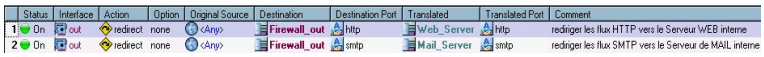
Exemple 5 : Redirection de port

Dans le cas où on ne possède qu'une seule adresse IP publique et plusieurs serveurs publics, la redirection de port permet de rediriger les flux à destination de ces serveurs en fonction uniquement du numéro de port.

Exemple

L'entreprise A possède l'adresse IP publique 192.36.253.240. Elle héberge un serveur Web et un serveur Mail dans la DMZ.

Le firewall va rediriger le flux vers le bon serveur en fonction du numéro de port visé. Si la demande de connexion concerne le port 80 (HTTP), le firewall redirige vers le serveur Web. Si la demande de connexion est faite sur le port 25 (SMTP), le firewall redirige le flux vers le serveur mail.


Status Interface Action Option Original Source Destination Destination Port Translated Translated Port Comment
1 On out redirect none <Any> Firewall_out http Web_Server http rediriger les flux HTTP vers le Serveur WEB interne
2 On out redirect none <Any> Firewall_out smtp Mail_Server smtp rediriger les flux SMTP vers le Serveur de MAIL interne

Remarque: Il est possible de rediriger le flux vers un autre port de la machine destination.

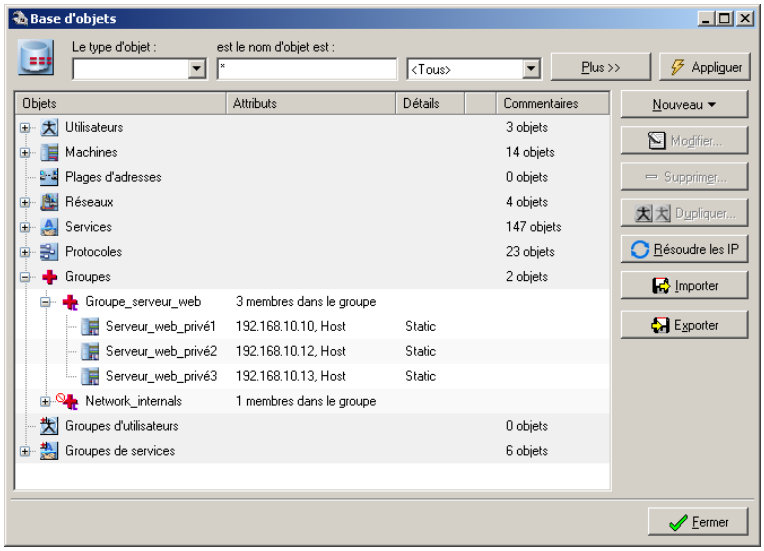
Exemple 6 : Partage de charge

Certains serveurs sont physiquement répliqués sur plusieurs machines pour pouvoir répondre plus efficacement au nombre important de connexions arrivant sur ces serveurs.

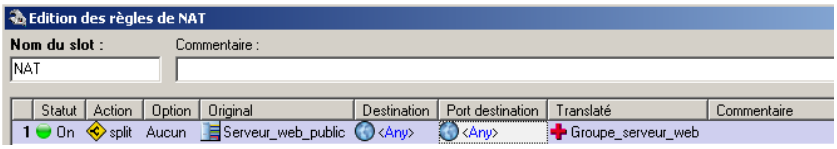
Avec le firewall NETASQ, il est possible que ces serveurs soient accessibles avec une seule adresse IP. Le firewall va rediriger vers les serveurs les demandes de connexions à destination de l'adresse IP publique.

Une entreprise A possède par exemple un serveur web (www.netasq.com), installé physiquement sur plusieurs machines dans la DMZ. La résolution DNS renvoie pour le site www.netasq.com, l'adresse IP 192.36.253.10.

On va créer un groupe de machines avec les adresses IP physiques des serveurs et donner une règle de translation au firewall.



Le flux à destination de l'adresse IP publique 192.36.253.10 est partagé équitablement et séquentiellement entre les différentes machines du groupe de serveurs web.


Edition des règles de NAT
Nom du slot :
NAT
Commentaire :
Statut Action Option Original Destination Port destination Translaté Commentaire
1 On split Aucun Serveur_web_public <Any> <Any> Groupe_serveur_web

Remarques

Il est possible de préciser les ports sources des machines source et destination en affichage détaillé. Cela revient à combiner partage de charge et redirection de ports.

Le partage se fait, dans cette version, de façon équitable, sans prise en compte de la charge respective des machines et/ou la disponibilité de ces machines.

Annexe E : Exemples de règles de filtrage

Dans cette annexe, nous vous indiquons concrètement comment configurer certaines règles de bases telles que :

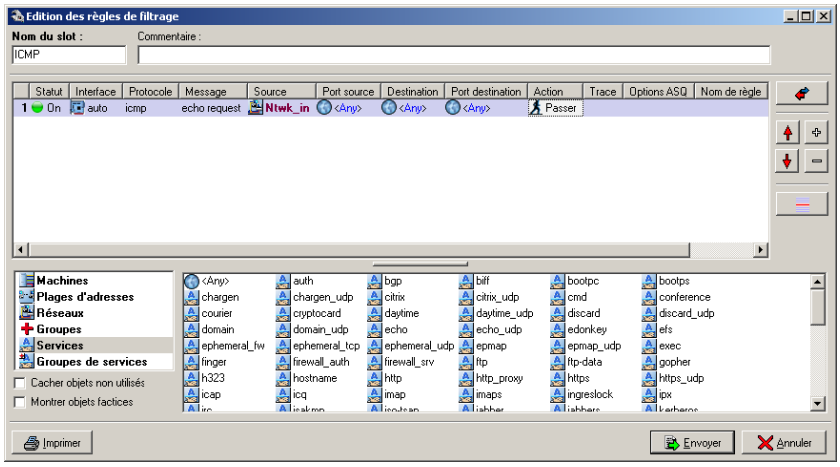
- ► Accès au DNS,
- ► Accès à ICMP,
- ► Accès au Telnet,
- ► Accès au FTP,
- ► Accès à un serveur Web interne depuis l'extérieur et depuis le réseau interne,
- ► Accès à l'internet avec ou sans le filtrage URL,
- ► Accès des postes clients au serveur mail,
- ► Configuration d'un serveur de messagerie,
- ► Régulation de bande passante,
- ► Vérification des règles de filtrage,
- ► Authentification

Certaines configurations peuvent s'avérer inutile si les règles implicites correspondantes ont été activées. (cf Chapitre X – Règles implicites).

Accès à ICMP

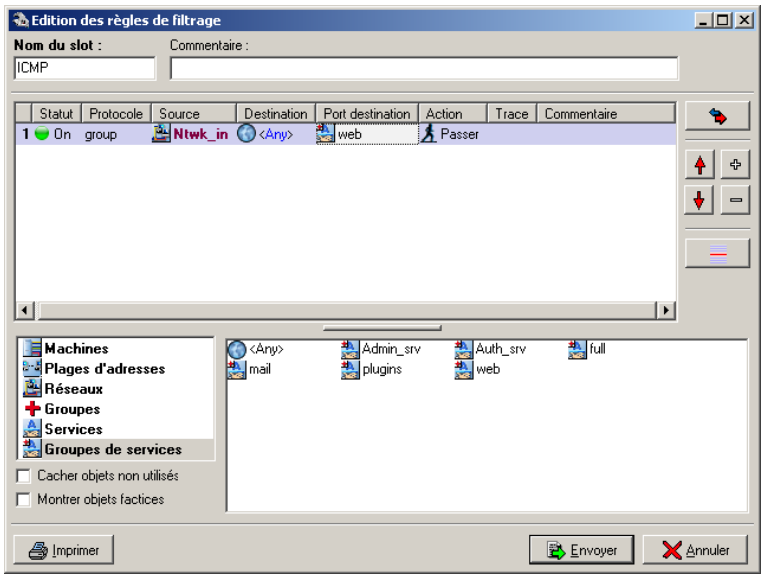
Dans cet exemple nous allons ajouter l'accès du réseau interne au protocole ICMP, permettant notamment d'utiliser le programme "ping".

Pour ajouter ICMP, il suffit, dans la sélection de services, de sélectionner "ICMP".



Vous pouvez, si vous le désirez n'autoriser que certains codes ICMP. Dans cet exemple, seul le ping (equo request) est autorisé.

Pour donner accès à l'Internet au réseau interne en passant par le Firewall, il suffit de mettre une règle qui autorise le réseau interne à contacter tout le monde en utilisant le protocole "http" et le protocole "domain_udp" pour la résolution DNS. Ces protocoles sont inclus au groupe de services "WEB".Cela donne :



Si vous utilisez le filtrage URL, vous allez passer indirectement par un proxy web situé sur le Firewall.

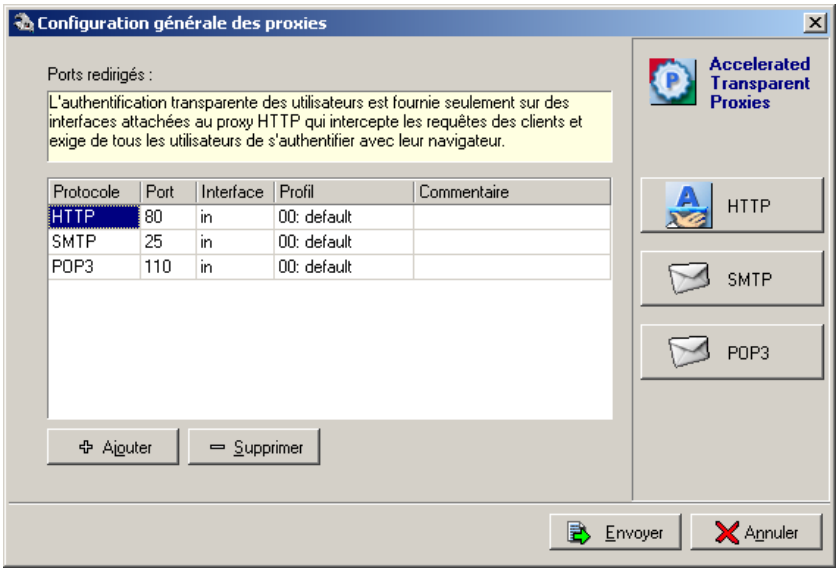
Vous ne vous connectez donc plus directement au serveur web mais au proxy web puis le proxy se connecte au serveur web. Ces différentes phases sont implicites dans les règles de filtrage.

Vous pouvez, au niveau des postes de travail, configurer votre navigateur pour vous connecter sur un serveur proxy distant. Dans ce cas, pour accéder à Internet, le poste n'utilise plus le protocole "http" sur le port 80 mais sur le port 8080.

Si vous avez implicitement laissé passer ce dernier protocole au niveau du Firewall, vos utilisateurs peuvent accéder à l'Internet sans passer par le filtrage d'URL que vous avez mis en place.

Pour éviter cela, vous pouvez rediriger toutes les requêtes utilisant un service particulier (8080 par exemple) vers le filtrage d'URL :

© Copyright NETASQ 2006

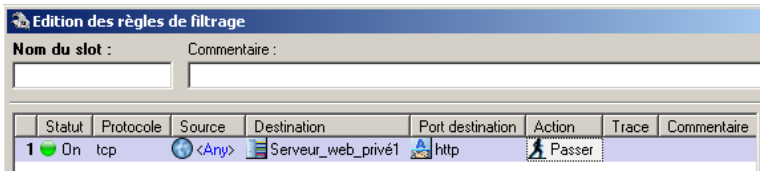

Configuration générale des proxies
Ports redirigés :
L'authentification transparente des utilisateurs est fournie seulement sur des interfaces attachées au proxy HTTP qui intercepte les requêtes des clients et exige de tous les utilisateurs de s'authentifier avec leur navigateur.
Accelerated Transparent Proxies
Protocole Port Interface Profil Commentaire
HTTP 80 in 00: default
SMTP 25 in 00: default
POP3 110 in 00: default
HTTP
SMTP
POP3
Ajouter
Supprimer
Envoyer
Annuler

Accès à un serveur WEB

Dans cet exemple, on suppose que votre serveur Web est disposé dans la DMZ.

Il doit être accessible depuis le réseau externe (depuis Internet) et depuis le réseau interne soit tout le monde.

La configuration du filtrage est alors assez simple : la machine source est "any", la machine destination est "Serveur_Web_prive1", le service "http" et l'action à appliquer est de "Passer" :


Edition des règles de filtrage
Nom du slot :
Commentaire :
Statut Protocole Source Destination Port destination Action Trace Commentaire
1 On tcp <Any> Serveur_web_privé1 http Passer

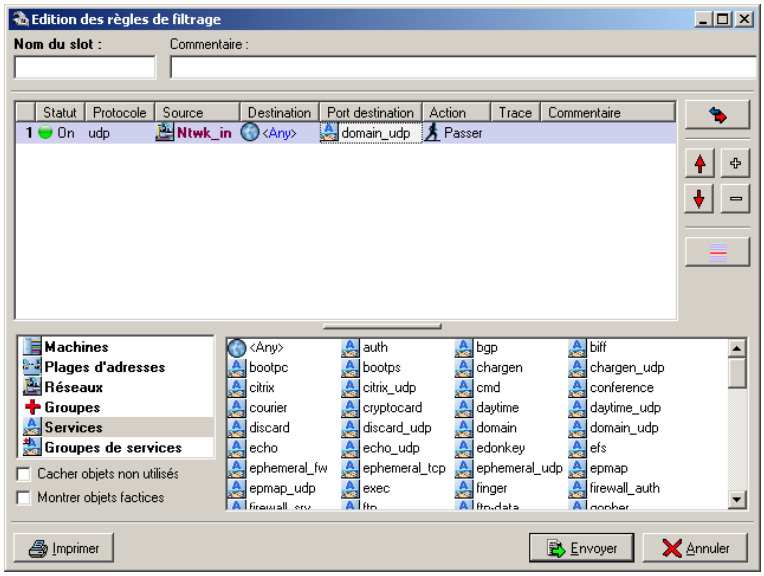
Si vous faîtes de la translation d'adresses pour ce serveur web, vous devez configurer une règle de translation supplémentaire pour y accéder de votre réseau interne avec son nom de domaine. Référez-vous à l'exemple sur la translation d'adresses traitant ce cas pour plus de renseignements.

Accès au DNS

Nous allons donner au réseau interne un accès au service DNS pour pouvoir utiliser les noms de domaine au lieu des adresses IP.

La règle suivante permet d'autoriser le réseau interne à accéder aux serveurs DNS (internes et externes). Il n'est pas nécessaire d'établir cette règle si vous avez choisi le groupe de services WEB, mais ce type de règle peut être intéressant si vous souhaitez filtrer les serveurs DNS accessibles.

© Copyright NETASQ 2006



Accès au FTP

Le protocole FTP est un peu particulier. Il utilise deux types de connexion :

► une connexion de commande pour envoyer et recevoir les commandes FTP,
► une connexion data pour le transit des flux de données.

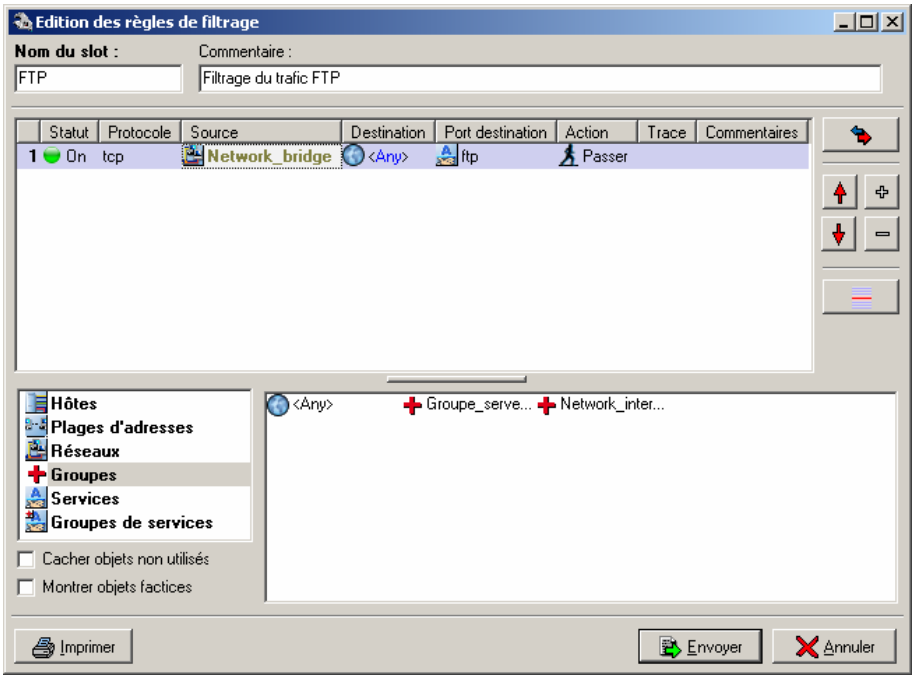
De plus le FTP peut être utilisé en deux modes différents :

► le FTP actif (sous DOS par exemple) pour lequel la connexion pour le transfert de données se fait par le port FTP-data du serveur . Cette connexion est à l'initiative du serveur. En FTP actif, l'adresse IP privée du client est envoyée, via la connexion de commande, au serveur afin que ce dernier puisse établir la seconde connexion. Si l'adresse privée du client est translatée, il faut donc cocher l'option "FTP actif" dans la configuration de la translation d'adresse, afin que le firewall modifie automatiquement l'adresse envoyée dans les commandes FTP.

► le FTP passif (avec un Browser Web par exemple), pour lequel la machine source effectue les deux connexions elle-même sur le serveur FTP. Cependant, le transfert de données ne se fait pas sur le port FTP-data mais sur un port éphémère du serveur.

Règle générale

Le firewall NETASQ intègre un plugin FTP qui va gérer automatiquement la seconde connexion (connexion data), vous permettant de ne définir qu'une seule règle de filtrage (celle pour autoriser la connexion de commande du client vers le serveur). La seule règle à définir est la suivante :



Cette règle permet à une machine du réseau interne (Network_Bridge) d'accéder aux serveurs FTP sur Internet.

Accès au serveur de messagerie placé en DMZ

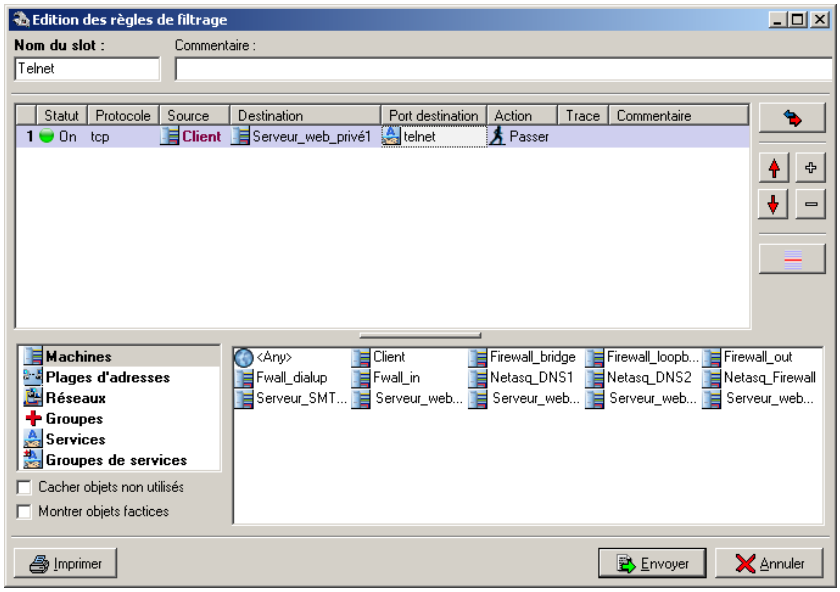
Pour pouvoir envoyer et recevoir des e-mails sur un poste client, il faut autoriser les services SMTP et POP3 du poste client vers le serveur de messagerie.

Le serveur de messagerie peut être un hébergé en interne ou à l'extérieur du réseau (chez le provider par exemple). Il faut donc déclarer, dans la configuration des objets, le serveur de messagerie (avec son adresse IP).

Vous pouvez ensuite créer un groupe de services appelé "Messagerie" dans lequel vous mettez les services POP3 et SMTP. Ceci vous évitera de mettre deux lignes possédant les mêmes propriétés dans les règles de filtrage.

Vous créez ensuite la règle de filtrage du réseau interne (où sont placés les postes clients) vers le serveur de Messagerie avec le groupe de Service « Messagerie » et l'action « Passer ». Cela donne :

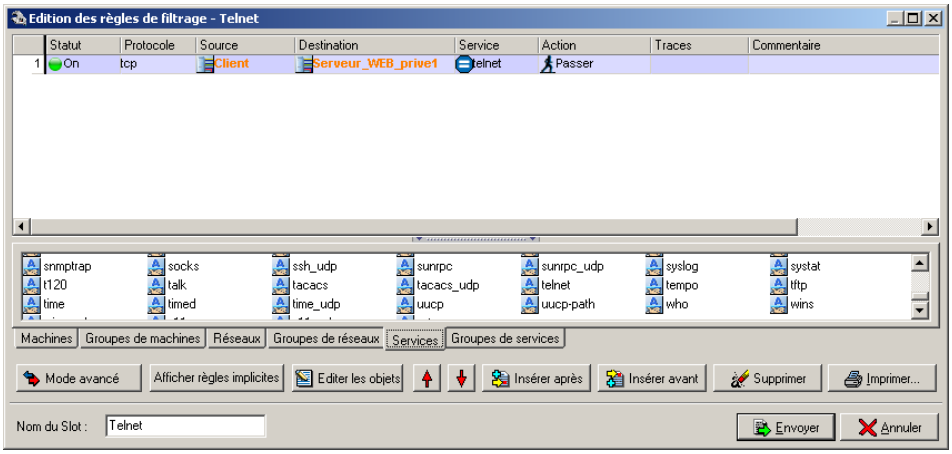
© Copyright NETASQ 2006



Accès au telnet

Le service telnet permet l'ouverture d'un shell sur une machine distante (généralement une machine UNIX).

Dans cet exemple, nous allons autoriser la machine « ma_machine » à se connecter au « mon_serveur_web » pour en assurer l'administration.



Seule la machine " Client " pourra faire un telnet sur le serveur Web, situé dans la DMZ.

Connexions IPSec

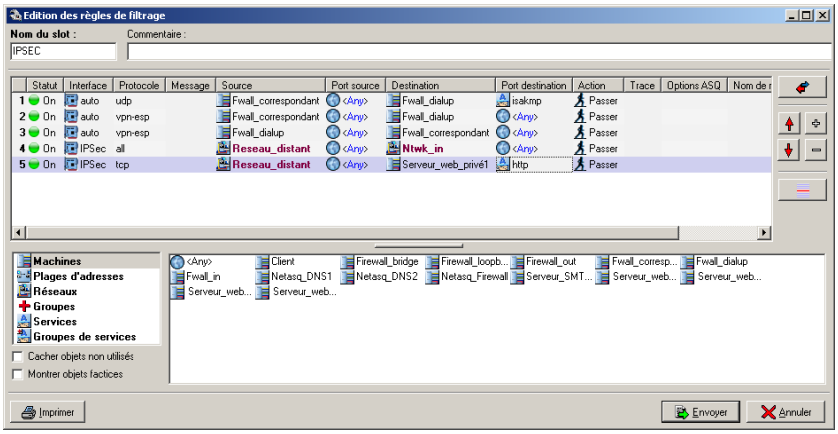
Après avoir paramétré le VPN IPsec sur le firewall, il faut mettre des règles de filtrage pour autoriser ces protocoles sur le firewall (sauf si les règles implicites sont activées pour ce type de trafic).

La première phase du protocole IKE se négocie sur le port UDP 500 (ISAKMP). Il faut donc autoriser les connexions sur ce port sur l'interface du firewall concernée par le tunnel.

Dans le cas d'une connexion IPsec sortante, il faut accepter une connexion sur un firewall distant sur le port ISAKMP.

En fonction des protocoles sélectionnés dans la configuration du VPN (ESP), il faut autoriser ces protocoles à atteindre le firewall. Ces règles ne sont pas prises en compte par le module Stateful Inspection et doivent donc être positionnées dans les deux sens de communications.

Les 3 premières règles de l'écran suivant permettent d'établir le tunnel VPN entre le firewall local et le firewall distant (ces 3 règles doivent être indiquées sur les deux firewalls réalisant le VPN). Pour un tunnel anonyme, l'objet « FW_correspondant » doit être remplacé par « ANY ».



Une fois les 3 premières règles en place, le tunnel peut être créé.

Vous pouvez ensuite filtrer les accès VPN aux machines internes. Pour filtrer les paquets arrivant au firewall au travers du tunnel, vous devez spécifier l'interface IPSEC (en affichage détaillé) pour définir les règles de filtrage. Pour filtrer les paquets sortant de votre firewall vers le tunnel VPN, vous n'avez pas besoin de définir l'interface (laissez l'interface sur auto) si les objets sources et destination sont bien précisés.

Les deux dernières règles indiquent comment filtrer les flux venant du réseau distant et passant par le VPN.

Connexions PPTP

Après avoir configurer le serveur PPTP sur le firewall, il faut mettre des règles de filtrage associées (sauf si les règles implicites sont activées pour ce type de trafic).

Vous avez besoin de rajouter trois règles :

► la première autorisant les clients PPTP à se connecter avec le protocole PPTP (TCP port 1723) sur l'interface du firewall utilisée pour le PPTP,

► deux autres autorisant le protocole GRE (protocole d'encapsulation) du client vers le firewall et la règle inverse.

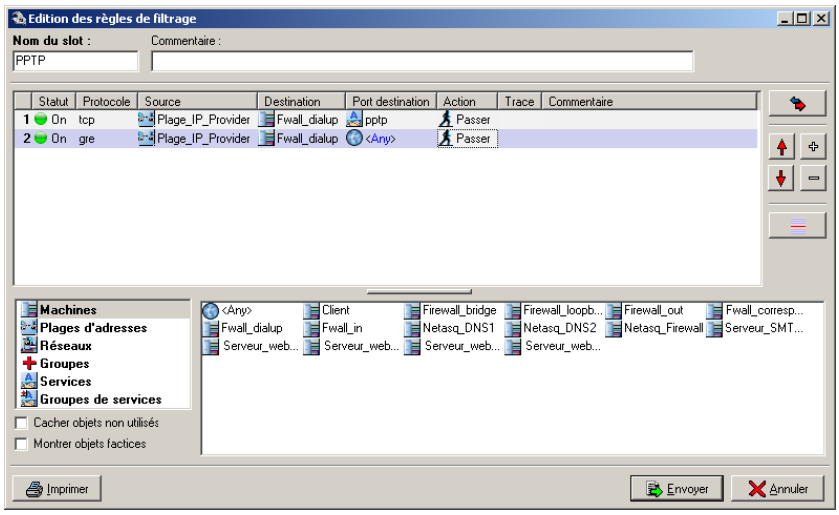
Exemple

On considère qu'un client se connecte sur Internet chez un provider A. Généralement, ce provider fournit des adresses IP dans une plage particulière qu'il est possible de repérer.

On crée donc un objet réseau Plage_IP_Provider avec ces adresses. Si vous ne connaissez pas cette plage, vous pouvez laisser l'objet « any » à la place.

On considère que la connexion Internet est relié à l'interface Out du firewall et les postes nomades arrivent sur cette interface pour se connecter en PPTP.

Les règles de filtrage sont donc, dans ce cas, les suivantes :



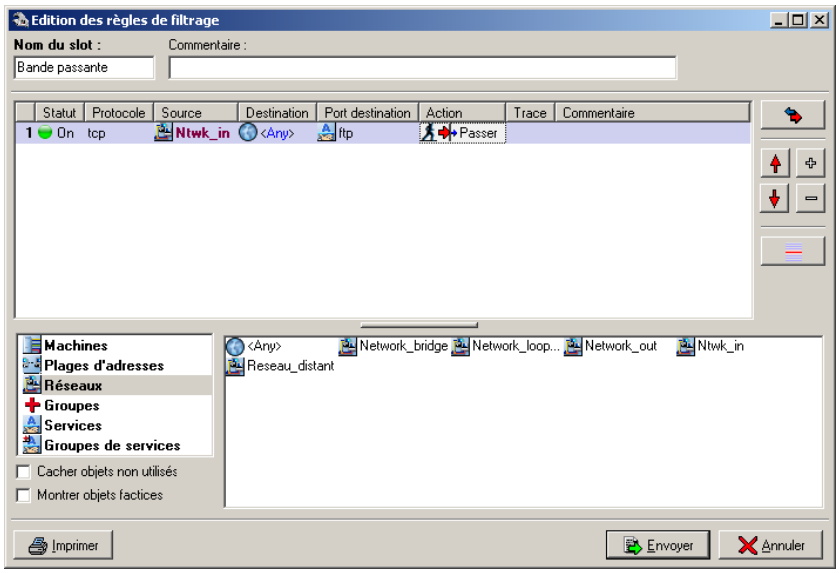
Contrôle de bande passante

Le Firewall NETASQ vous donne la possibilité de faire de la régulation de bande passante. Ceci se fait en autorisant le passage d'un nombre limité d'octets pendant une période de 1 seconde.

Le niveau peut être assez fin puisque vous pouvez limiter chacun des services du protocole IP, pour chaque machine différente.

Ceci se paramètre au niveau du filtrage par l'action "Limiter à". Au lieu de bloquer ou laisser passer les paquets, ils vont être autorisés jusqu'au seuil fixé puis se verront rejetés si le seuil est atteint dans la période donnée.

L'exemple ci-dessous illustre comment limiter le téléchargement de fichiers en FTP à partir du réseau interne.



Contrôle du filtrage

Après avoir configuré les règles les plus simples, il se peut que vous vous demandiez s'il n'en manque pas pour assurer le bon fonctionnement des flux réseaux.

Il se peut aussi qu'un serveur applicatif utilise un protocole particulier que vous ne connaissez pas.

Si vous n'utilisez pas de règles explicitement bloquantes pour ces machines ou protocoles, un moyen simple est de placer temporairement une règle de traçage en fin de filtrage. Cette règle va logger tout ce qui est bloqué par le firewall.

Ainsi, le flux que vous n'avez pas explicitement autorisé passe toutes les règles puis arrive en fin de tableau où il subit la règle par défaut (bloquer). Si vous placez une règle qui trace tout juste avant la règle par défaut (qui n'apparaît pas dans la liste des règles de filtrage), le flux sera inscrit dans les fichiers de traces que vous pourrez consulter ensuite.

Vous verrez notamment apparaître, dans le fichier de trace, le numéro de port destination, ce qui est utile si vous ne le connaissiez pas.

Vous pouvez aussi analyser tout ce qui a été bloqué et voir si certains flux doivent réellement être bloqués.

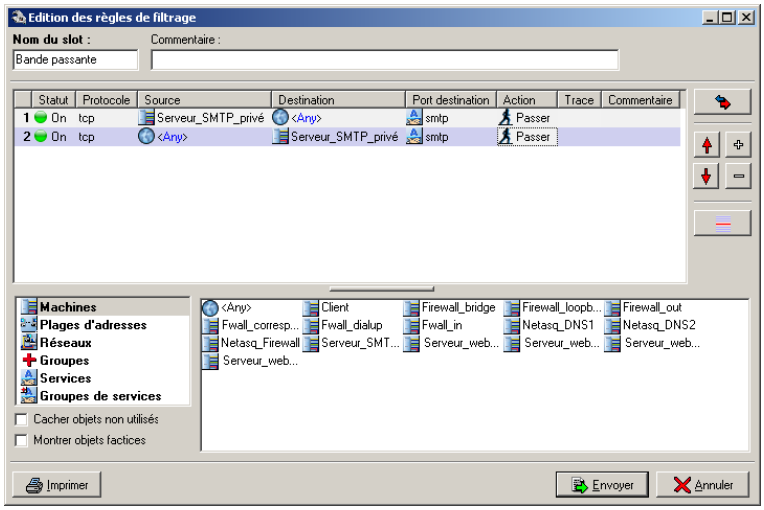
Accès au serveur de messagerie

Si vous possédez votre propre serveur de messagerie, il faut, au niveau du filtrage, lui autoriser l'envoi et la réception des courriers. Pour cela, il suffit d'autoriser l'envoi et la réception au travers du service SMTP.

Ceci n'est bien entendu utile que si votre serveur de messagerie communique avec l'extérieur. S'il sert uniquement pour la messagerie interne, ces règles sont inutiles.

Le serveur de messagerie envoie ou reçoit des courriers de différents serveurs de messagerie, qui ne sont pas identifiables. Ils seront donc représentés par la machine "any".

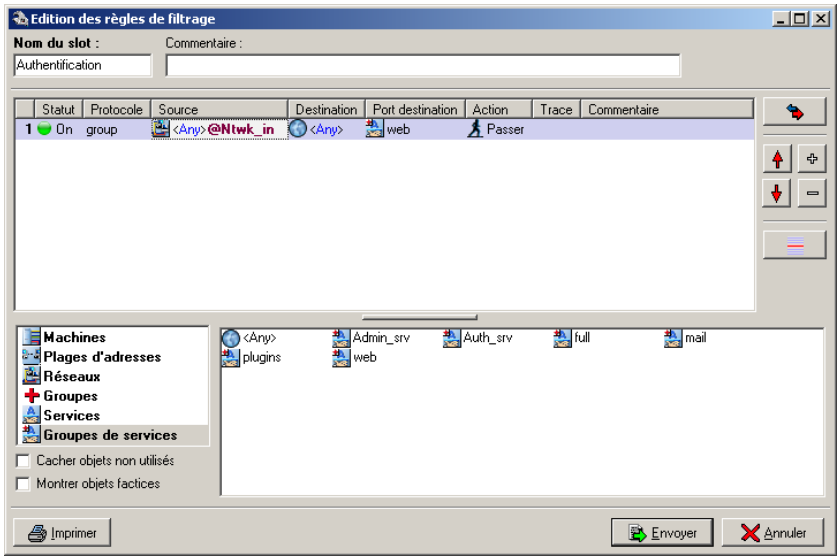
Les deux règles (une pour l'émission l'autre pour la réception) sont les suivantes :



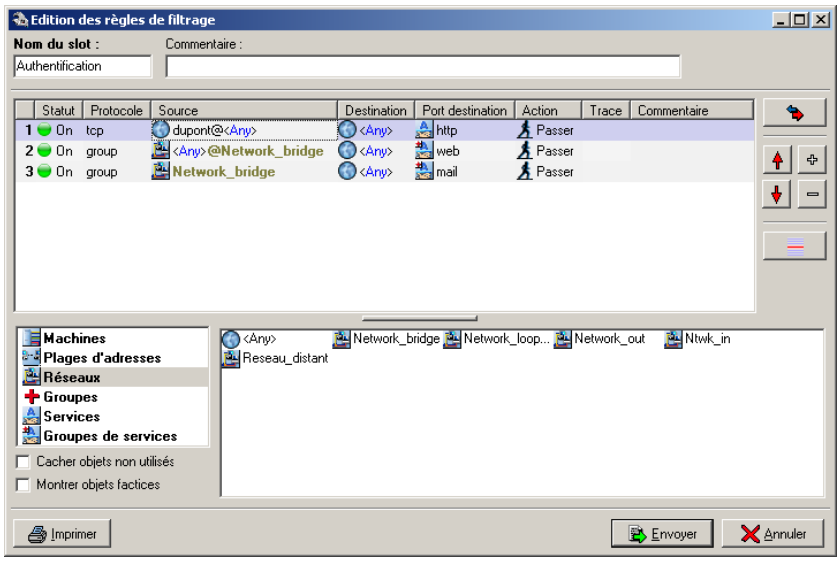
Remarques : si votre serveur de messagerie est juste un relais avec le serveur de messagerie de votre provider Internet, l'échange se fait uniquement du port 25 (SMTP) vers le port 25 de votre serveur.

Authentification

L'authentification peut être demandée pour l'accès à certains services ou à certaines machines. Pour cela, il faut avoir défini les fiches des utilisateurs qui peuvent s'authentifier au travers du firewall. Par exemple, l'accès au WEB pour les utilisateurs authentifiés, appartenant au réseau interne, pourra être autorisé avec la règle suivante :



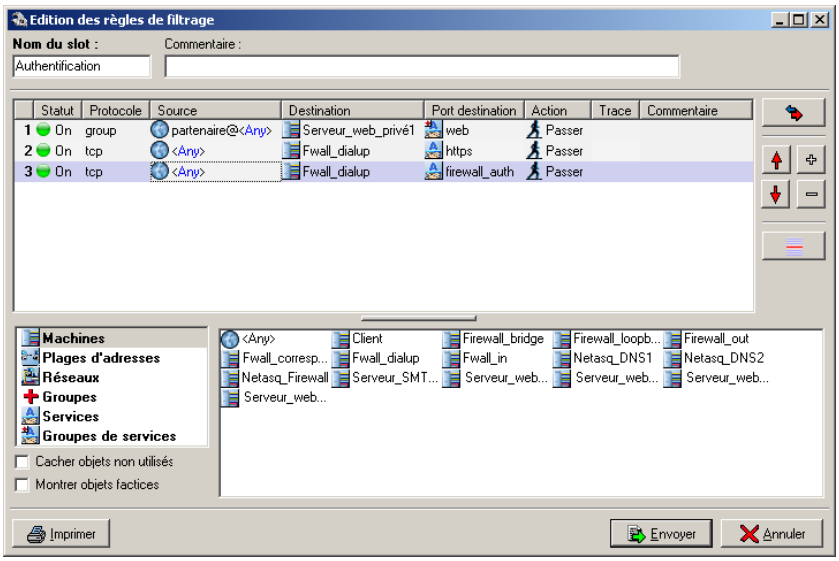
Vous pouvez aussi donner des accès particuliers à certains utilisateurs authentifiés. Par exemple, la politique suivante autorise l'utilisateur DUPONT à faire du FTP (où qu'il se trouve), les utilisateurs authentifiés du réseau Network_bridge peuvent faire du WEB et tous les utilisateurs du réseau Network_bridge, même non authentifiés, ont accès à la messagerie :



Il est aussi possible d'authentifier les utilisateurs pour des connexions entrantes (provenant de l'Internet).

Ainsi, vous pouvez autoriser l'accès à certains services hébergés sur votre réseau interne à certains utilisateurs de l'Internet (il faut bien entendu que les informations de connexion aient été, au

préalable, fournies à ces utilisateurs). L'exemple suivant montre comment autoriser le groupe d'utilisateur Partenaire à accéder à un serveur WEB particulier (pour un Extranet, par exemple) :



Si vous souhaitez authentifier des utilisateurs situés à l'extérieur du périmètre de sécurité du firewall, il faut autoriser les services nécessaires à l'authentification, à savoir le service HTTPS et le service d'authentification propriétaire NETASQ via SRP (port1200). Attention, le port 1200 ne doit être ouvert que si vous utilisez l'authentification via SRP, dans les autres cas seul le HTTPS est nécessaire.

Annexe F : Evénements

Voici une liste non exhaustive des notifications d'événements déclenchés par le Firewall NETASQ.

Notification d'événements

Certains événements sont logués par le firewall sans être pour autant des attaques. Ces événements sont visualisable à partir du Firewall Manager (Menu "Configuration" "Traces").

Notification	Description
Arrêt du firewall	Indique un arrêt du firewall
authentification échouée pour + nom d'utilisateur	L'authentification du protocole PPTP a échoué (le login ou le mot de passe PPTP sont incorrects).
connexion terminée pour + nom d'utilisateur	La connexion PPTP ou dialup est terminée.
Il reste 20% d'espace libre pour le fichier de log	Le fichier de log a dépassé les 80% de remplissage (seulement en mode shutdown ou sécurisation, ce qui signifie que dans ce cas le firewall agit comme un « block all »).
connexion établie pour	La connexion PPTP ou dialup est correctement établie.
phase 1 IPsec échouée	La phase 1 du protocole IKE n'a pas pu s'établir correctement.
phase 2 IPsec échouée	La phase 2 du protocole IKE n'a pas pu s'établir correctement.
la clé IPsec est introuvable pour + identifiant VPN	Aucune clé pré-partagée ne correspond à cet identifiant VPN. La clé correspondant à l'identifiant n'a pas été définie dans le gestionnaire des clés pré-partagées.
démarrage du firewall	Indique un démarrage du firewall.
HA : Défaillance du firewall actif	Indique une panne du firewall actif. Le firewall passif devient alors actif. (Cet événement ne peut-être détecté que si vous possédez deux firewalls configurés en haute disponibilité).
HA: Défaillance du firewall passif	Indique une panne du firewall passif (Cet événement ne peut-être détecté que si vous possédez deux firewalls configurés en haute disponibilité).
CRL invalide pour le tunnel VPN	La liste de révocation de certificats (CRL) utilisée pour un tunnel VPN n'est pas valide.
certificat invalide pour le tunnel VPN	Le certificat de l'équipement VPN distant n'est pas valide.
La partition de log a changé	La partition disque contenant les logs n'est plus détectée sur le même disque qu'au précédent reboot. Deux causes sont possibles : une intervention matérielle (un disque a été rajouté dans le firewall pour contenir la partition de log), un problème disque (la partition de log n'est plus correctement détectée).

Annexe G : Foire aux questions

1. Que signifie le message "Impossible de localiser la machine en x.x.x.x" ?
2. Comment vérifier l'(les) adresse(s) IP réellement affectée(s) au firewall ?
3. Que signifie le message "Vous avez perdu le privilège MODIFY" ?
4. Que signifie le message "L'opération a dépassé le temps imparti" ?
5. Comment arrêter le voyant d'alarme majeure sur le firewall ?
6. Comment suis-je au courant d'une tentative d'intrusion ?
7. Que se passe-t-il lorsqu'une alarme est déclenchée par le firewall ?
8. Est-il possible de laisser passer d'autres protocoles que IP ?

1. Que signifie le message "Impossible de localiser la machine en x.x.x.x" ?

Ce message signifie que la machine sur laquelle vous êtes connecté ne peut pas joindre le firewall avec l'adresse IP que vous avez précisée dans la fenêtre de connexion. Le problème peut être dû à plusieurs choses.

Vérifiez:

► Que l'adresse IP que vous avez spécifiée dans la fenêtre de connexion est bien celle du firewall (celle de l'interface interne en mode avancé),
► Que votre machine possède bien une adresse IP différente du firewall mais dans le même sous-réseau,
► Que les branchements sont corrects (utilisez un câble croisé uniquement si vous branchez le firewall directement à une machine ou un routeur). Tapez "arp -a" dans une fenêtre DOS sous Windows pour voir si le PC connaît l'adresse physique (Ethernet) du Firewall NETASQ. Si ce n'est pas le cas, vérifier vos câbles, les connexions physiques à votre hub,
► Que vous n'avez pas changé de mode de fonctionnement du firewall (transparent ou avancé),
► Que l'adresse IP est bien prise en compte au niveau du firewall (cf Comment vérifier l'adresse IP affectée au firewall),
► Que le serveur d'accès à l'interface graphique n'a pas été désactivé sur le firewall.

2. Comment vérifier l'(les) adresse(s) IP réellement affectée(s) au firewall ?

Afin de vérifier la(les) adresse(s) IP affectée(s) au firewall ainsi que le mode de fonctionnement, il suffit de se connecter en mode console au firewall. Pour cela, vous pouvez soit faire un SSH sur le firewall (si le SSH est activé et autorisé), soit vous connecter directement sur le boîtier par le port série ou en branchant un écran et un clavier sur le boîtier.

Une fois connecté en mode console (avec le login admin ou root), tapez la commande *« ifinfo »* Le résultat vous donne la configuration des cartes réseau et le mode de fonctionnement actuel.

3. Que signifie le message "Vous avez perdu le privilège MODIFY" ?

Il ne peut y avoir qu'un seul utilisateur ayant les droits de modification connecté au firewall. Ce message signifie qu'une session est ouverte par un utilisateur ayant le droit de modification.

© Copyright NETASQ 2006

Pour forcer la fermeture de cette session, il suffit de se connecter en ajoutant un point d'exclamation devant le nom d'utilisateur (!admin).

Attention, si une session avec le droit MODIFY est ouverte sur une autre machine, elle sera fermée.

4. Que signifie le message "L'opération a dépassé le temps imparti" ?

Par mesure de sécurité, toute connexion, aboutie ou non, entre le firewall et l'interface graphique est stoppée au bout d'un certain temps. Cela évite notamment d'attendre indéfiniment la connexion dans le cas où le firewall n'est pas joignable sur le réseau.

5. Comment arrêter le voyant d'alarme majeure sur le firewall ?

La led d'alarme majeure s'allume dès qu'une alarme majeure est reçue et reste allumée tant que personne ne valide la visualisation de l'alarme.

Pour arrêter la led, il suffit de valider l'option « Eteindre les LEDs » dans le menu firewall.

6. Comment suis-je au courant d'une tentative d'intrusion ?

Chaque tentative d'intrusion déclenche une alarme majeure ou mineure suivant son importance. Vous êtes informés de ces alarmes par quatre moyens différents :

► Premièrement, les leds sur la face avant du boîtier s'allument (rouge) ou clignotent (jaune) pour vous signaler l'alarme,

► Ensuite, les alarmes sont tracées dans un fichier spécifique consultable à partir de l'interface graphique (Firewall Monitor ou Reporter),

► Vous pouvez recevoir un rapport d'alarmes à une fréquence régulière (cf réception des alarmes),

► Enfin, le Firewall Monitor affiche à l'écran, en temps réel, les alarmes reçues.

7. Que se passe-t-il lorsqu'une alarme est déclenchée par le firewall ?

Toute tentative d'intrusion ou attaque détectée est automatiquement stoppée. Suivant la configuration, les paquets qui déclenchent une alarme au niveau du firewall est soit bloqué soit stoppé.

En cas d'attaque franche, il convient de surveiller de près les connections entrantes à l'aide du Firewall Monitor ou Reporter ou d'autres outils d'analyse réseau.

8. Est-il possible de laisser passer d'autres protocoles que IP ?

Le firewall NETASQ ne peut filtrer que les protocoles fonctionnant sur IP. Tout autre protocole qui n'est pas reconnu par le firewall est considérer comme suspect et se retrouve bloqué.

Cependant, avec le mode de fonctionnement transparent, il est possible de laisser passer d'autres protocoles sans les filtrer. Ces protocoles sont IPX de Novell, IPv6, PPPoE, Appletalk et Netbios.

L'accès au firewall en mode console (connexion par SSH, par port série ou avec un écran-clavier) permet la maintenance du firewall au moyen d'un jeu de commandes.

Cette annexe présente les principales commandes utilisées (attention à bien respecter la casse) :

Lancement du serveur de commandes

► **nsrpc user@127.0.0.1** : permet de lancer, de façon locale, le serveur de commande du firewall avec le user admin.

Visualisation d'informations de configuration

► **ifinfo :** affiche la correspondance entre les noms des interfaces définies dans la configuration réseau (avec le Firewall Manager) et les noms utilisés par le système.
► **ifconfig** : affiche les informations relatives à la configuration réseau du firewall.
► **ipnat -l :** donne les règles de translation d'adresses actives.
► **sfctl -s filter** : donnes les règles de filtrage actives.
► **netstat -rn** : affiche la table de routage du firewall.

Vous avez la possibilité de visualiser le contenu des fichiers de configuration avec un éditeur tel que vi.

Les fichiers de configuration se trouvent dans le répertoire /Firewall/ConfigFiles.

Activation/Désactivation de slot ou de fonctionnalité

Désactivation

► **ennat 00 :** désactive les translations d'adresses.
► **envpn 00** : désactive le tunnel VPN actif.
► **enurl 00 :** désactive le filtrage d'URL.

Activation

► **ennat xx :** active le slot de translation d'adresses portant le numéro xx.
► **envpn xx :** active le slot vpn portant le numéro xx.
► **enurl xx :** active le slot de filtrage d'URL portant le numéro xx.
► **enfilter xx :** active le slot de filtrage portant le numéro xx.
► **enfilter 10 :** active le slot 10 (pass_all dans la configuration par défaut, le firewall laisse passer tous les paquets).
► **endialup :** relance une connexion avec un modem.
► **ennetwork :** recharge une configuration réseau.
► **engui :** réactive l'autorisation de connexion du Firewall Manager sur les réseaux internes.

Activité du firewall

► **sfctl -s stat :** donne les statistiques du firewall.
► **sfctl –T :** affiche des informations « temps réel » sur le moteur stateful du firewall,
► **dstat :** donne la liste des services actifs.
► **top -u :** donne l'activité du processeur et des processus ainsi que l'occupation de la mémoire.
► **tcpdump -i <nom de l'interface> <filtre> :** affiche en temps réels les paquets qui transitent par une interface du firewall.

► <*nom de l'interface*> correspond au nom de l'interface utilisé par le système (ce nom peut être récupéré grâce à la commande ifinfo)
► <*filtre*> permet de filtrer les protocoles ou services affichés.

© Copyright NETASQ 2006

Le filtre d'un service doit être précédé du mot "port". Les services peuvent être indiqués par leur numéro de port ou par leur nom (si le service fait partie des services courants).

Exemple de filtres

► tcpdump -i fxp0 not port 23 (pour ne pas afficher les flux telnet),
► tcpdump -i fxp0 udp OR port HTTP (pour n'afficher que les flux UDP et HTTP),
► tcpdump -i fxp0 tcp AND port 53(pour n'afficher que les flux DNS TCP),
► tcpdump –s0 –w /tmp/dump –i fxp0 (écriture du trafic dans un fichier donné),
► tcpdump –s0 –i fxp0 ESP OR port isakmp (visualisation du trafic chiffré ESP ou des phases de négociation VPN).

Commandes VPN

► **showSPD :** Affichage de la SPD (Security Policy Database) contenant toutes les informations relatives aux tunnels définis (actifs ou non).
► **showSAD :** Affichage de la SAD (Security Association Database) contenant les informations relatives aux tunnels actifs.

Divers

► **getversion :** affiche la version logicielle du firewall.

Utilisez cette commande dès la réception de votre IPS-Firewall pour vérifier que la version livrée correspond bien à la version attendue.

La manipulation des fichiers et l'utilisation de certaines commandes doivent être réalisées avec précaution, en effet certaines opérations peuvent avoir des conséquences sur le fonctionnement du firewall.

Support technique et « sysinfo »

Enfin la commande « sysinfo » permet la visualisation de la configuration complète d'un appliance UTM NETASQ. Indispensables à la bonne compréhension de votre problème, les informations fournies par cette commande vous sont systématiquement demandées par le support technique lors de la résolution d'un incident.

Pour information, le résultat de cette commande peut être obtenu par l'intermédiaire du menu « Firewall \ Support technique NETASQ » du Firewall Manager. Ce menu permet notamment l'enregistrement du résultat pour envoi au support par exemple.

Ci-dessous, est présenté un exemple (partiel) du résultat de la commande sysinfo.

```
##############################
#  Software information   #
##############################
current date :  2006-07-18 18:42:42
Serial      :  F200XA118450999999
Model       :  F200-A
Software    :  Netasq Firewall software version 6.2.1
Branch/Build :  EUROPE / M
Partitions   :  Active=Main BackupVersion="6.2.1" BackupBranch=" EUROPE " Date="2006-07-11
14:42:39" Boot=Main
Uptime      :  36 days 3:52, hours
##############################

##############################
#  Slot information       #
##############################
Filtering : slot_filter_01
NAT       : slot_nat
VPN       : slot_vpn
```

```
URL      :
##############################

##############################
#   Memory information      #
##############################
Stateful
--------

host                        0 %
fragment                      0 %
ICMP                        0 %
connection                    0 %
data tracking                 0 %

mbuf
----
1012/1056/7798 mbufs in use (current/peak/max):
       1012 mbufs allocated to data
261/272/5199 mbuf clusters in use (current/peak/max)
808 Kbytes allocated to network (6% of mb_map in use)
0 requests for memory denied
0 requests for memory delayed
0 calls to protocol drain routines
```

Annexe I : Rôle de la DMZ

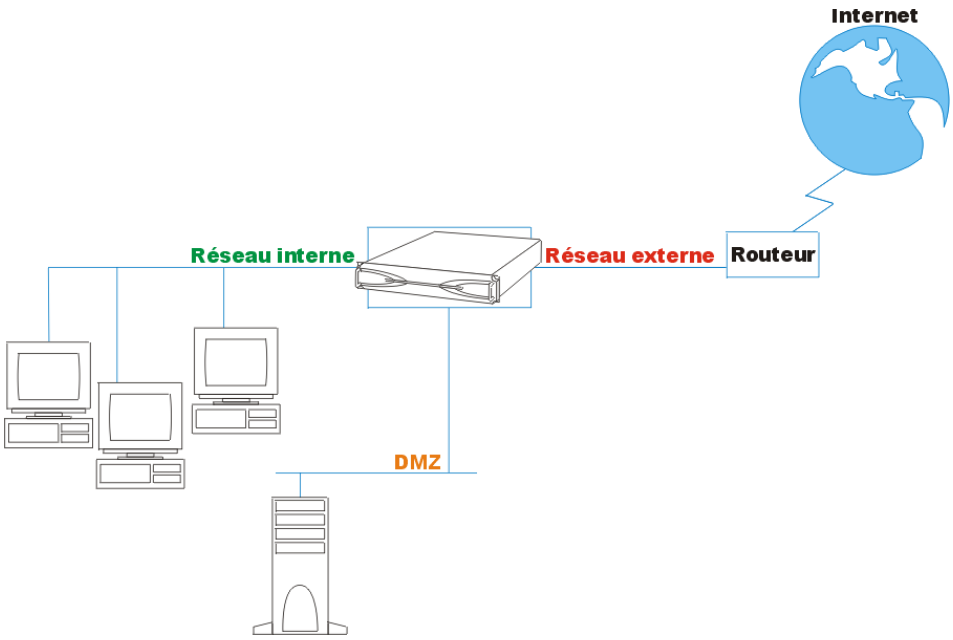
Le but habituel d'une DMZ (De-Militarized Zone) est d'isoler de votre réseau interne les machines qui doivent recevoir des connexions du monde extérieur.

Ainsi, vous isolez complètement l'accès direct du réseau externe vers votre réseau interne. Les accès possibles de l'extérieur se font uniquement dans la DMZ qui est physiquement séparée du réseau interne.

Vous bénéficiez ainsi d'une protection efficace sur le réseau interne. Les machines de la DMZ, qui sont exposées à un risque plus important (puisque joignables de l'extérieur), ne peuvent pas permettre de rebondir directement sur l'ensemble du réseau.

Il faut ensuite bien définir les relations entre la DMZ et le réseau interne pour ne pas compromettre le niveau de sécurité atteint.

Exemple de mise en place d'une DMZ



La DMZ peut aussi être utilisée à d'autres fins (séparation de branches d'une entreprise,...)

Annexe J : Connexion au serveur SSH

Le firewall NETASQ intègre un serveur SSH. La connexion à ce serveur peut servir à la configuration du firewall en mode console (en ligne de commande).

Définition de Secure Shell

Secure Shell est un protocole de communication sécurisé permettant l'accès distant au Firewall afin d'y exécuter des programmes. SSH permet de pallier les faiblesses de sécurité des accès distants tels que telnet en fournissant les services de sécurité essentiels : authentification du serveur et du client, confidentialité des flux (notamment des mots de passe).

SSH repose sur la technique de cryptographie asymétrique RSA pour l'authentification et utilise l'algorithme symétrique IDEA pour la confidentialité des flux.

Activation du serveur SSH sur le Firewall

Le service est désactivé par défaut sur le Firewall, il faut donc l'activer par l'intermédiaire du menu « Firewall > Sécurité ».

La clé privée de l'utilisateur admin sera nécessaire pour l'authentification lors de la connexion. Il est donc nécessaire de la sauvegarder et de la stocker dans un répertoire sur la machine depuis laquelle la connexion en SSH sera lancée.

Par défaut le filtrage du firewall bloque la connexion sur le port 22 (SSH) du Firewall. Il est donc nécessaire de mettre en place une règle de filtrage pour autoriser cette communication.

Configuration de la partie cliente

Un logiciel ssh supportant la version 2 de ce protocole est nécessaire pour l'utilisation avec le firewall.

La configuration de la partie cliente dépend du logiciel client utilisé.

© Copyright NETASQ 2006

Annexe K : Activation Key

Votre IPS-Firewall NETASQ vous a peut être été vendu avec une carte nommée Activation Key.

Principe

Les Activation Key sont des cartes, au format carte de crédit, contenant des informations susceptibles de modifier logiciellement la licence des produits NETASQ. Une carte n'est utilisable qu'une seule fois : une fois qu'une Activation Key est associée à un numéro de série d'appliance NETASQ, elle ne peut plus être affectée à un autre appliance.

Comment se présente une carte ?

La carte se présente de la façon suivante :

Face Avant **Face Arrière**

Activation Key
NETASQ
Secure Internet Connectivity
www.netasq.com
Activation Key
This card enables the modification of a NETASQ product's licence, according to the reference stated below.
Modification has to be done via NETASQ's Website.
Cette carte permet de modifier la licence d'un produit NETASQ, en fonction de la référence ci-dessous.
La modification doit être réalisée via le site WEB de NETASQ.
REFERENCE :
SERIAL NUMBER :
CODE :
NETASQ - 3 rue Archimède
59650 Villeneuve d'Ascq - France
WEB Site : www.netasq.com
NETASQ

Sur la face arrière, 3 informations sont indiquées :

- la *référence* de l'Activation Key,
- le *serial number* de l'Activation Key,
- le *code* de l'Activation Key.

Ces deux dernières informations sont nécessaires pour modifier la licence du produit en adéquation avec la référence de l'Activation Key.

Comment activer la carte ?

Pour activer une Activation Key et donc modifier en conséquence la licence d'un produit, connectez-vous sur le site WEB de NETASQ : www.netasq.fr.

L'activation de l'Activation Key peut être réalisée en même temps que le téléchargement initial de la licence ou peut être réalisé ultérieurement.

Comme pour le téléchargement initial de la licence, veuillez effectuer les opérations suivantes :

1. Dirigez-vous dans la section « **Espace client** ».
   Indiquez alors votre numéro de support, obtenu après la phase d'enregistrement du boîtier et votre mot de passe WEB.

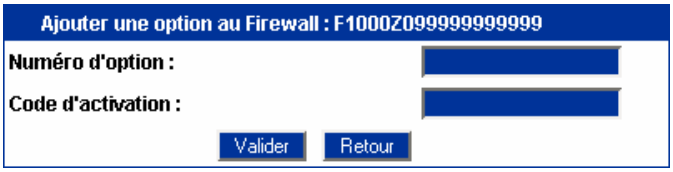
© Copyright NETASQ 2006

2. Vous arrivez alors dans votre espace personnel. Dans la section « Centre de téléchargement », sélectionnez « Téléchargement de licence ».

3. La liste des licences des produits enregistrés sur votre espace client s'affiche. Cliquez sur le lien « Détails » qui correspond au boîtier pour lequel vous désirez activer la carte, dans la colonne Licence.

4. Une page descriptive des caractéristiques du produit s'affiche.

5. Cliquez sur le bouton « Ajouter une option ». Le tableau suivant apparaît :



Indiquez ensuite le numéro d'option (serial number) et le code d'activation de la carte. Une validation vous sera demandée avant l'activation effective de l'option. La nouvelle licence sera disponible sous un délai de 20 minutes (un mail de confirmation vous sera alors envoyé à l'adresse que vous avez indiqué lors de l'enregistrement).

Pendant ce délai, vous pouvez télécharger une licence temporaire vous permettant d'utiliser le produit (mais les options correspondant aux Activation Key ne seront pas actives), en choisissant la version logicielle de votre produit puis en cliquant sur le bouton « **Téléchargement licence »** (voir descriptif des caractéristiques). Le numéro de version logicielle est donné lors de l'installation de l'interface graphique d'administration des appliances NETASQ (disponible sur le CDROM livré avec le produit).

Lorsque votre licence définitive sera disponible, reprenez les étapes 1, 2 et 3 puis cliquez sur le bouton « **Téléchargement licence** ».

Comment activer une architecture haute disponibilité ?

Pour activer deux boîtiers en haute disponibilité, la procédure à suivre est décrite ci-dessous :

Etapes	Actions
1	Enregistrez les deux produits utilisés pour monter l'architecture haute disponibilité.
2	Dans la liste des boîtiers présentés dans votre espace personnel, choisissez alors le boîtier « Maître ». Le boîtier « Maître » correspond au boîtier principal, pour lequel l'option Haute disponibilité a la valeur « None » (Cette information peut être visualisée dans le détail de la licence, voir descriptif des caractéristiques du produit).
3	Activez, sur le boîtier « Maître », toutes les Activation Key

	commandées pour la solution haute disponibilité (conformément au tableau de procédure précédent), exceptée la carte portant la référence : NA-HA.
4	Une fois toutes les Activation Key activées sur le boîtier Maître, activez de la même façon, la carte NA-HA. Vous devez alors indiquer le numéro de série du boîtier « Slave » (second boîtier utilisé pour l'architecture Haute disponibilité. Attention, ce boîtier doit obligatoirement avoir la valeur « Slave » pour l'option Haute disponibilité, comme indiqué sur le détail de la licence, voir descriptif des caractéristiques du produit). La licence du boîtier « Slave » sera alors automatiquement copiée à partir de la licence du boîtier « Maître » et l'option Haute disponibilité prendra la valeur « Master » sur le boîtier « Maître ».
5	Les nouvelles licences pour les deux boîtiers seront disponibles sous un délai de 20 minutes (un mail de confirmation vous sera alors envoyé à l'adresse que vous avez indiquée lors de l'enregistrement).

Annexe L : Réinitialisation de l'IPS-Firewall

Il est possible de restaurer la configuration usine d'un IPS-Firewall NETASQ. Cette opération raméne alors le produit dans l'état où il était à la livraison.

La réinitialisation d'un IPS-Firewall détruit toute la configuration réalisée sur le produit, excepté le mot de passe (voir ci-dessous). Elle est irreversible, attention donc à ne réaliser cette opération que si elle est absolument nécessaire.

Pour le F50, l'opération entraîne aussi la réinitialisation du mot de passe. Pour les autres produits, la réinitialisation garde le mot de passe en vigueur. Donc même après une réinitialisation, l'IPS-Firewall est toujours accessible avec le même mot de passe. Il n'est pas possible de réinitialiser le mot de passe de votre IPS-Firewall (sauf F50) avec la procédure décrite ici.

Cas du F25 et F50

Pour réinitialiser le F25 ou F50, retournez le boîtier et munissez-vous d'une pointe (stylo bille par exemple). Un petit interrupteur est placé sous le boîtier et est accessible par un trou réalisé dans le capôt. Maintenez l'interrupteur appuyé au moyen de la pointe pendant plusieurs secondes (environ 15 secondes) jusqu'à entendre un signal sonore. La procédure de réinitialisation de l'IPS-Firewall se lancera alors automatiquement et après quelques instants l'IPS-Firewall aura retrouvé sa configuration d'usine et rebootera. Ce reboot peut durer 5 minutes, veuillez donc attendre la fin du reboot (nouveau signal sonore) pour vous reconnecter à l'IPS-Firewall Attention, cette opération réinitialise aussi le mot de passe.

Pour tous les autres produits

Pour les autres produits, la réinitialisation du boîtier se fait en mode console. Plusieurs méthodes permettent d'accèder à l'IPS-Firewall en mode console, la plus simple est réalisée avec la liaison série. Pour cela, utilisez le câble série livré avec l'IPS-Firewall pour connecter l'appliance et un PC via leur port série respectif.

Lancez ensuite une application du type HyperTerminal (accessible via le menu « Démarrer > Programmes > Accessoires > Communication »).

Choisissez alors une comunication sur le port « COM », puis spécifiez les paramètres du port suivants :

Bits par seconde : 9600
Bits de données : 8
Parité : Aucun
Bits d'arrêt : 1
Contrôle de flux : Matériel

L'invite suivante apparaît alors :

FreeBSD (F2003D099999999999) (ttyd0)
login :

Renseignez alors le login « admin » puis le mot de passe correspondant au login « admin » que vous utilisez d'habitude pour vous connecter à l'IPS-Firewall. Vous êtes maintenant connecté à l'IPS-Firewall. Tapez alors la commande : « defaultconfig –f » et appuyez sur entrée.

```
FreeBSD (F2003D099999999999) (ttyd0)
login: admin
SSH Passphrase:
Copyright (c) 1980, 1983, 1986,1988, 1990, 1991, 1993, 1994
                The Regents of the University of California. All rights reserved

F2003D099999999999>defaultconfig -f
```

Un bip d'avertissement doit retentir et votre IPS-Firewall doit rebooter. Le IPS-Firewall est alors réinitialisé.

Annexe M : Noms interdits

Voici une liste des noms d'objets (à l'exception des objets « utilisateur ») interdits sur l' IPS-Firewall NETASQ. :

Caractères interdits

Ces caractères ne peuvent être utilisés dans les noms d'objets :

- « »
- \
- #
- @
- [
-]
- =
- <tab>
- <espace>

Caractères interdits en première position

Les noms d'objets ne peuvent commencer par les chiffres (0, 1, 2, 3, 4, 5, 6, 7, 8, 9).

Préfixes interdits

Ces préfixes, non sensibles à la casse, ne peuvent être utilisés en début d'un nom d'objet :

- Firewall_
- Network_
- ephemeral_
- Global_

Nom interdits

Les noms suivants, non sensibles à la casse, ne peuvent pas être utilisés dans la création d'objets sur l'IPS-Firewall :

- any
- anonymous
- broadcast

© Copyright NETASQ 2006

Annexe N : Fichiers de traces NETASQ

Le traitement des flux de trafics transitant par les IPS-Firewalls entraîne la génération d'enregistrements d'audit contenant un descriptif de tous les événements rencontrés. Suivant les types des événements rencontrés, ceux-ci font l'objet d'un enregistrement dans des fichiers de traces NETASQ spécifiques.

Il existe ainsi treize (13) types de fichiers de traces disponibles sur les IPS-Firewalls NETASQ : web, smtp, connection, filter, alarm, plugins, auth, server, vpn, filterstat, natstat, count et system.

Les noms utilisés pour ces fichiers de traces sont explicites :

► **« web »** est utilisé pour les traces des trafics WEB, ce fichier est renseigné par le proxy HTTP,

Exemple : le proxy de l'IPS-Firewall a enregistré la requête de l'utilisateur « jean.dupont » à destination du site WEB « www.netasq.com ».

► **« smtp »** est utilisé pour les traces du trafic SMTP, ce fichier est renseigné par le proxy SMTP,

Exemple : le proxy de l'IPS-Firewall a enregistré l'envoi d'un mail de l'utilisateur « jean.dupont@netasq.com » à destination de « pierre.durand@netasq.com ».

► **« connection »** est utilisé pour les connexions à travers et à destination de l'IPS-Firewall, ce fichier est renseigné par le moteur IPS NETASQ, l'ASQ,

Exemple : le noyau ASQ de l'IPS-Firewall a enregistré la connexion de la machine « 192.168.0.2 » et du port « 1672 » à destination de la machine « 192.168.1.2 » et du port « 1840 ».

► **« filter »** est utilisé pour les traces générées par le filtrage (une entrée est inscrite à chaque fois qu'une règle de filtrage possédant l'attribut « Tracer » est associé à un trafic transitant par l'IPS-Firewall), ce fichier est renseigné par le moteur IPS NETASQ, l'ASQ,

Exemple : le noyau ASQ de l'IPS-Firewall a enregistré que la règle de filtrage « 3 » (possédant l'attribut « tracer ») a été utilisée pour le traitement d'un paquet transitant par l'IPS-Firewall.

Les informations enregistrées dans ce fichier de traces sont les suivantes :

Firewall	Numéro de série de l'IPS-Firewall ou Nom (si connu).
Date	Date de génération de l'enregistrement.
Heure	Heure de génération de l'enregistrement.
Fuseau	Fuseau horaire de l'IPS-Firewall.
Enregistré à	Heure d'enregistrement de l'événement.
Règle ID	Identifiant de la règle.
Interface source	Carte réseau de l'Interface Source.
Nom Interface src	Nom de l'Interface Source (uniquement si connu).
Interface Dst	Carte réseau de l'interface Destination.
Nom Interface Dst	Nom de l'interface Destination (uniquement si connu).
Protocole	Protocole analysé ou Port Destination.

© Copyright NETASQ 2006

Protocole Internet	Protocole IP.
Type ICMP	Type du message (uniquement si ICMP).
Code ICMP	Code du message (uniquement si ICMP).
Source	Adresse IP de la source.
Nom Source	Nom de la source (uniquement si connu).
Utilisateur	Nom de l'utilisateur authentifié.
Destination	Adresse IP de la destination.
Nom Destination	Nom de la destination (uniquement si connu).
Port Source	Numéro de port de la source (uniquement si TCP/UDP).
Nom Port Source	Nom du port de la source (uniquement si connu).
Port Destination	Numéro du port de la destination (uniquement si TCP/UDP).
Nom Port Dst	Nom du port de la destination (uniquement si connu).
Action	Action de la règle de filtrage.

► **« alarm »** est utilisé pour les alarmes remontées par l'ASQ des IPS-Firewalls (les règles de filtrage et les événements « Système » possédant un attribut « Mineure » ou « Majeure » sont enregistrées dans ce fichier), ce fichier est renseigné par le moteur IPS NETASQ, l'ASQ,

Exemple : le noyau ASQ de l'IPS-Firewall a enregistré une tentative de rebond FTP sur un serveur FTP protégé par l'IPS-Firewall (ce trafic est bloqué par défaut et remonte une alarme mineure).

Firewall	Numéro de série de l'IPS-Firewall ou Nom (si connu).
Date	Date de génération de l'enregistrement.
Heure	Heure de génération de l'enregistrement.
Fuseau	Fuseau horaire de l'IPS-Firewall.
Enregistré à	Heure d'enregistrement de l'événement.
Priorité	Pour les alarmes, niveau de l'alarme (majeur ou mineur).
Règle ID	Identifiant de la règle.
Interface source	Carte réseau de l'Interface Source.
Nom Interface src	Nom de l'Interface Source (uniquement si connu).
Protocole	Protocole analysé ou Port Destination.
Protocole Internet	Protocole IP.
Type ICMP	Type du message (uniquement si ICMP).
Code ICMP	Code du message (uniquement si ICMP).
Source	Adresse IP de la source.
Nom Source	Nom de la source (uniquement si connu).
Utilisateur	Nom de l'utilisateur authentifié.

Destination	Adresse IP de la destination.
Nom Destination	Nom de la destination (uniquement si connu).
Port Source	Numéro de port de la source (uniquement si TCP/UDP).
Nom Port Source	Nom du port de la source (uniquement si connu).
Port Destination	Numéro du port de la destination (uniquement si TCP/UDP).
Nom Port Dst	Nom du port de la destination (uniquement si connu).
Action	Action de la règle de filtrage.
Message	Informations complémentaires sur l'alarme.
Aide	Accès à une aide compléméntaire sur l'alarme.

► **« plugins »** est utilisé pour les traitements des plugins de l'ASQ, ce fichier est renseigné par le moteur IPS NETASQ, l'ASQ,

Exemple : le noyau ASQ de l'IPS-Firewall a enregistré une requête HTTP anormalement formée (dépassement du nombre de caractères autorisés dans l'URL de la requête).

► **« auth »** est utilisé pour les traitements de l'authentification sur les IPS-Firewalls, ce fichier est renseigné par le processus de gestion de l'authentification,

Exemple : le module d'authentification de l'IPS-Firewall a enregistré l'authentification de l'utilisateur « jean.dupont » pour une période de quatre (4) heures.

Date Heure	Date et heure de génération de l'enregistrement.
User	Identifiant de l'utilisateur demandant à être authentifié.
Source	Adresse source de la connexion.
Destination	Adresse destination de la connexion.
Status	Code d'erreur de retour de la demande.
Message	Message de retour de la demande.

► **« server »** est utilisé pour le fonctionnement du serveur d'administration des IPS-Firewalls : « serverd » (dans ce fichier se trouve listé toutes commandes envoyées au serverd pour la configuration des IPS-Firewalls, potentiellement on peut y retrouver toutes les commandes de configuration des IPS-Firewalls. Ces commandes sont aussi utilisées pour la configuration en ligne de commandes des IPS-Firewalls), ce fichier est renseigné par le serveur d'administration « serverd »,

Exemple : le module d'administration de l'IPS-Firewall a enregistré la commande « config asq alarm show » visant à afficher la configuration des alarmes de l'ASQ.

Date	Date et heure de génération de l'enregistrement.
User	Identité de l'administrateur (login).
Address	Adresse IP source de la connexion.
Session	Format 00.0000. Les deux premiers chiffres correspondent au nombre de réinitialisations, les quatres suivants correspondent au nombre de connexions.
Status	Code d'erreur de retour de la commande.
Message	Ligne de commande envoyée à l'IPS-Firewall.

► **« vpn »** est utilisé pour les événements associés aux politiques VPN.

Exemple : le module VPN a enregistré la création d'un tunnel VPN entre les passerelles « 192.168.12.35 » et « 47.89.69.215 ».

Date Heure	Date et heure de génération de l'enregistrement.
Niveau d'erreur	Message d'erreur.
Phase	Phase de négociation de la SA.
Source	Adresse source de la connexion.
Destination	Adresse destination de la connexion.
Message	Message concernant la tentative de mise en place d'un tunnel.

► **« filterstat »** est utilisé pour afficher des statistiques sur le filtrage, ce fichier est renseigné par le processus firewall,

Exemple : le système de l'IPS-Firewall a enregistré que 1205 octets de trafic UDP, 52 octets de trafic ICMP et 4879 octets de trafic TCP ont transité à travers l'IPS-Firewall entre le 5 juillet 2004 00:00:00 et le 15 août 2004 23:59:59.

► **« natstat »** est utilisé pour afficher des statistiques sur la translation d'adresses, ce fichier est renseigné par le processus firewall,

Exemple : le système de l'IPS-Firewall a enregistré le nombre de translations d'adresses réalisées vers le réseau interne, vers l'extérieur, la règle de translation utilisée...

► **« count »** est utilisé pour afficher des statistiques de comptage (principalement dans le cas des règles de filtrage possédant l'attribut « Compter »), ce fichier est renseigné par le processus firewall,

Exemple : le système de l'IPS-Firewall a enregistré que la règle de filtrage « 4 » (possédant l'attribut « Compter ») a été utilisée 68501 durant la période sélectionnée.

► **« system »** est utilisé pour le fonctionnement de certains processus des IPS-Firewalls (les événements « Système » possédant un attribut « System » sont enregistrés dans ce fichier), ce fichier est renseigné par plusieurs processus de l'IPS-Firewall (services DNS, DHCP, etc).

Exemple : l'IPS-Firewall a enregistré le démarrage du module d'authentification des IPS-Firewalls.

Date	Date et heure de génération de l'enregistrement.
Service	Service associé au message.
Message	Message associé à l'enregistrement.

Comme indiqué ci-dessus les quatre fichiers de traces principaux sont renseignés par le processus central de tous les IPS-Firewalls NETASQ, l'ASQ. Parmi ces fichiers, celui qui apparaît le plus important est sans conteste le fichier « alarm » qui tient compte des événements illégaux (non relatif au filtrage) associés à des attaques contre le système.

Attention, la classification des traces est présentée ici selon un point de vue « Système ». Tandis que certaines modifications sont réalisées pour l'affichage des traces dans les logiciels de la suite d'administration NETASQ. Par exemple les traces correspondant aux trafics WEB sont présentées dans la section Fichier > WEB du Reporter. Ces traces correspondent au fichier « web » et aux traces associées au plugin HTTP dans le fichier « plugin ».

Les fichiers de logs sont des fichiers texte. Un log correspond à une ligne terminée par les caractères 0D et 0A (en hexadécimal).

Les lignes sont au format standard WELF. Un document décrivant ce format peut être trouvé sur le site de webtrends : http://www.webtrends.com/library/prtnr_welf.doc.

Paquets bloqués et Paquets permis

Dans chaque ligne de traces, il est important de repérer le token « Action ». Ce token permet d'identifier les paquets qui ont été autorisés (par la politique de filtrage ou parce qu'ils n'ont pas été bloqués par les analyses de l'ASQ) lorsque sa valeur est « pass » et les paquets qui ont été bloqués (soit ils ont été supprimés silencieusement par l'IPS-Firewall soit ils ont été supprimés et une réinitialisation a été envoyé à la machine source de ce paquet, cette information n'est pas disponible pour les administrateurs de l'IPS-Firewall) lorsque sa valeur est « block ».

Traces de modification de l'heure des IPS-Firewalls.

Lorsque un IPS-Firewall est remis à l'heure, une ligne spéciale est écrite dans tous les fichiers de traces.Elle se présente comme ceci :

id=firewall time="2003-12-29 16:35:32"fw="F1003C006000100401"tz=+0100 startime="2003-12-29 16:30:10"datechange=1 duration=322

Le token « datechange=1 » signifie qu'il s'agit d'une remise à l'heure et « duration » spécifie le nombre de secondes de décalage.

Exceptions sur les tokens

Certains fichiers de traces ne suivent pas exactement le format standard WELF. Ces exceptions sont répertoriées dans la section suivante.

Exceptions communes a tous les logs

« rule »est remplacé par ruleid,
le token « time » désigne l'heure d'enregistrement de la ligne dans le fichier de log à l'heure locale du firewall,
« tz » désigne le décalage selon le fuseau horaire du firewall au moment ou il écrit le log.On peut donc connaître l'heure du log selon le temps universel et analyser une attaque survenant simultanément sur des équipements répartis dans des pays différents,
« startime » désigne l'heure du début d'une connexion. Si une connexion dure une heure « time » sera au moins égal à « startime» plus une heure,
« groupid » représente une session complète FTP,on retrouve cette notion dans les logs de plugin,
« dstif » ,« srcif »,« dstifname »,« srcifname » désignent les interfaces source et destination du firewall avec leur noms,
« user » correspond dans plusieurs logs à des noms de personnes authentifiées via « authd »,
« icmptype » et « icmpcode » correspondent au type et au code icmp dans les logs d'alarmes.

Journal SMTP

« user » correspond à l'envoyeur du mail et « dstname » correspond au destinataire.

Journal SERVER

« error » est un entier commençant à zéro qui exprime respectivement : OK, LAST (dernière commande), FAILED (echec de la commande), AUTH_FAILED (echec de l'authentification), LEVEL_DENIED (les droits de l'utilisateurs ne permettent pas cette commande),
« user » correspond à la personne connectée par serverd (et non pas dans ce cas a une personne authentifiée).
« address »est l'adresse IP se connectant via serverd au Firewall.
« sessionid » est un entier correspondant a un numéro attribué lors d'une session.Lorsqu'il y a plusieurs connexions simultanées cela permet de distinguer les différentes sessions.

© Copyright NETASQ 2006

« msg »: on retrouve chaque commande passée par le client. Les informations sensibles telles que les mots de passe sont retirées.

Journal AUTH

Dans « user » on retrouve la personne ayant tenté ou s''étant authentifiée,
« method »correspond à la méthode utilisée pour s'authentifier, se référer au document de l'authentification,
« msg » contient un texte explicitant le nombre d'heures allouées,
« error »est un entier qui exprime 0 vaut OK, 2 vaut FAILED (echec de l'authentification).

Journal SYSTEM

Les proxies y écrivent aussi ses événements propre a son fonctionnement.

« service »correspond au nom du service écrivain.
« msg » explicite l'action du service ayant généré ce log.

Journal FILTERSTAT

Les tokens commençant par « Rule » suivi d'un entier correspondant a l'indice d'une régle. La valeur associée représente le nombre de fois que la règle a concordé.

Par exemple Rule0=1661 : la règle 0 a concordé 1661 fois.

SavedEvaluation : nombre d'évaluations de règles n'ayant pas dû être faites grace à la technologie ASQ,
HostMem : Mémoire allouée pour un hote,
FragMem : Mémoire allouée pour les fragments,
ICMPMem : Mémoire allouée pour l'icmp,
ConnMem : Mémoire allouée pour les connexions,
Logged : Nombre de lignes de logs générées par l'ASQ,
LogOverflow : Nombre de lignes de logs perdues (génération impossible par l'ASQ),
Accepted : Nombre de paquets concordant aux règles passantes,
Blocked : Nombre de paquets concordant aux règles bloquantes,
Byte : Nombre d'octets ayant transité par le firewall,
Fragmented : Nombre de paquets fragmentés ayant transité par le firewall,
TCPPacket : Nombre de paquets TCP ayant transité par le firewall,
TCPByte : Nombre d'octets de paquets TCP ayant transité par le firewall,
TCPConn : Nombre de connexion TCP ayant transité par le firewall,
UDPPacket : Nombre de paquets UDP ayant transité par le firewall,
UDPByte : Nombre d'octets de paquets UDP ayant transité par le firewall,
UDPConn : Nombre de connexion UDP ayant transité par le firewall,
ICMPPacket : Nombre de paquets ICMP ayant transité par le firewall,
ICMPByte : Nombre d'octets de paquets ICMP ayant transité par le firewall.

Journal NATSTAT

Les tokens spécifiques sont :

mappedin :nombre de paquets translatés en entrée,
mappedout :nombre de paquets translatés en sortie,
added :nombre de nouvelles sessions actives,
expired :timeout,nombre de sessions expirees,
memfail :paquets ne pouvant etre translates car on a atteint la taille max de la table de sessions actives,
badnat :paquets non translates (echec de la creation de nouvelles sessions),
inuse :nombre de sessions actives,
rules :nombre de règles de NAT actives.

Journal COUNT

Les tokens commençant par « Rule » suivi d'un entier correspondant à l'indice d'une régle. La valeur associée représente le nombre de fois que la règle a concordé.

Par exemple Rule0=1661 : la règle 0 a concordé 1661 fois.

© Copyright NETASQ 2006

© Copyright NETASQ 2006

ISC-DHCP

Copyright (c) 2004-2005 by Internet Systems Consortium, Inc. ("ISC")
Copyright (c) 1995-2003 by Internet Software Consortium
#
Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.
#
THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES
WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS.IN NO EVENT SHALL ISC BE LIABLE FOR
ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT
OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
#
#Internet Systems Consortium, Inc.
#950 Charter Street
#Redwood City, CA 94063
#<info@isc.org>
#http://www.isc.org/

MPL-1.1

MOZILLA PUBLIC LICENSE
Version 1.1

---

1. Definitions.

1.0.1. "Commercial Use" means distribution or otherwise making the Covered Code available to a third party.

1.1. "Contributor" means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable" means Covered Code in any form other than Source Code.

1.6. "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License" means this document.

1.8.1. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is: A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

B. Any new file that contains any part of the Original Code or previous Modifications.

1.10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation,method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your")means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1.
For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1. The Initial Developer Grant.
The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a)under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

(b) under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

(c) the licenses granted in this Section 2.1(a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

(d) Notwithstanding Section 2.1(b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code;or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant.
Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

(a)under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using, or selling ofModifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1)

Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

(c) the licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

(d)Notwithstanding Section 2.2(b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2)separate from the Contributor Version;
3)for infringements caused by: i) third party modifications of Contributor Version or ii)the combination of Modifications made by that Contributor with other software(except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Application of License.
The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code.
Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications.
You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters
(a) Third Party Claims.
If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs.
If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c)Representations.
Contributor represents that, except as disclosed pursuant to Section 3.4(a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code.If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice.If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A.You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code.You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions.
You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works.
You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6. Versions of the License.

6.1. New Versions.
Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions.
Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3. Derivative Works.
If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any

confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED CODE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED CODE IS WITH YOU. SHOULD ANY COVERED CODE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8. TERMINATION.

8.1.This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2.If You initiate litigation by asserting a patent infringement claim (excluding declatory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant")alleging that:

(a)such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant.If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

(b)any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3.If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4.In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN

INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10. U.S. GOVERNMENT END USERS.

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. MISCELLANEOUS.

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. MULTIPLE-LICENSED CODE.

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed"."Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the NPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

EXHIBIT A -Mozilla Public License.

``The contents of this file are subject to the Mozilla Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.mozilla.org/MPL/

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____.
Portions created by _____ are Copyright (C) _____
_____. All Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms of the _____ license (the"[___] License"), in which case the provisions of [_____] License are applicable instead of those above.If you wish to allow use of your version of this file only under the terms of the [____] License and not to allow others to use your version of this file under the MPL, indicate your decision by deletingthe

provisions above and replacethem with the notice and other provisions required by the [___] License.If you do not delete the provisions above, a recipient may use your version of this file under either the MPL or the [___] License."

[NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.]

HEIMDAL

```
/*
 Copyright (c) 1997-2003 Kungliga Tekniska Hogskolan
 (Royal Institute of Technology, Stockholm, Sweden).
 All rights reserved.
 *
 Redistribution and use in source and binary forms, with or without
 modification, are permitted provided that the following conditions
 are met:
 *
 1. Redistributions of source code must retain the above copyright
 *notice, this list of conditions and the following disclaimer.
 *
 2. Redistributions in binary form must reproduce the above copyright
 *notice, this list of conditions and the following disclaimer in the
 *documentation and/or other materials provided with the distribution.
 *
 3. Neither the name of the Institute nor the names of its contributors
 *may be used to endorse or promote products derived from this software
 *without specific prior written permission.
 *
 THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS ``AS IS'' AND
 ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE
 ARE DISCLAIMED.IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE
 FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 SUCH DAMAGE.
 */
```

BONNIE++

```
 COPYRIGHT NOTICE:
 Copyright (c) Tim Bray <tbray@textuality.com>, 1990.
 Copyright (c) Russell Coker <russell@coker.com.au>, 1999.
 Everybody is hereby granted rights to use, copy, and modify this program,
provided only that this copyright notice and the disclaimer below
are preserved without change.
 DISCLAIMER:
 This program is provided AS IS with no warranty of any kind, and
 The author makes no representation with respect to the adequacy of this
program for any particular purpose or with respect to its adequacy to
produce any particular result, and
 The author shall not be liable for loss or damage arising out of
the use of this program regardless of how sustained, and
 In no event shall the author be liable for special, direct, indirect
or consequential damage, loss, costs or fees or expenses of any
nature or kind.
```

OPENLDAP

Copyright 1998-2005 The OpenLDAP Foundation All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License.

A copy of this license is available in the file LICENSE in the top-level directory of the distribution or, alternatively, at <http://www.OpenLDAP.org/license.html>.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Individual files and/or contributed packages may be copyright by other parties and subject to additional restrictions.

This work is derived from the University of Michigan LDAP v3.3 distribution.Information concerning this software is available at <http://www.umich.edu/~dirsvcs/ldap/>.

This work also contains materials derived from public sources.

Additional information about OpenLDAP can be obtained at <http://www.openldap.org/>.

Portions Copyright 1998-2004 Kurt D. Zeilenga.
Portions Copyright 1998-2004 Net Boolean Incorporated.
Portions Copyright 2001-2004 IBM Corporation.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License.

Portions Copyright 1999-2003 Howard Y.H. Chu.
Portions Copyright 1999-2003 Symas Corporation.
Portions Copyright 1998-2003 Hallvard B. Furuseth.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that this notice is preserved. The names of the copyright holders may not be used to endorse or promote products derived from this software without their specific prior written permission.This software is provided ``as is'' without express or implied warranty.

Portions Copyright (c) 1992-1996 Regents of the University of Michigan. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor.The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.This software is provided ``as is'' without express or implied warranty.

GPLv1

GNU GENERAL PUBLIC LICENSE
Version 1, February 1989

Copyright (C) 1989 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The license agreements of most software companies try to keep users at the mercy of those companies.By contrast, our General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.The General Public License applies to the Free Software Foundation's software and to any other program whose authors commit to using it. You can use it for your programs, too.

When we speak of free software, we are referring to freedom, not price.Specifically, the General Public License is designed to make sure that you have the freedom to give away or sell copies of free software, that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of a such a program, whether gratis or for a fee, you must give the recipients all the rights that you have.You must make sure that they, too, receive or can get the source code.And you must tell them their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software.If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License.The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any work containing the Program or a portion of it, either verbatim or with modifications.Each licensee is addressed as "you".

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this General Public License and to the absence of any warranty; and give any other recipients of the Program a copy of this General Public License along with the Program.You may charge a fee for the physical act of transferring a copy.

2. You may modify your copy or copies of the Program or any portion of it, and copy and distribute such modifications under the terms of Paragraph 1 above, provided that you also do the following:

a) cause the modified files to carry prominent notices stating that you changed the files and the date of any change; and

b) cause the whole of any work that you distribute or publish, that in whole or in part contains the Program or any part thereof, either with or without modifications, to be licensed at no charge to all third parties under the terms of this General Public License (except that you may choose to grant warranty protection to some or all third parties, at your option).

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the simplest and most usual way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty

(or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this General Public License.

d) You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

Mere aggregation of another independent work with the Program (or its derivative) on a volume of a storage or distribution medium does not bring the other work under the scope of these terms.

3. You may copy and distribute the Program (or a portion or derivative of it, under Paragraph 2) in object code or executable form under the terms of Paragraphs 1 and 2 above provided that you also do one of the following:

a) accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Paragraphs 1 and 2 above; or,

b) accompany it with a written offer, valid for at least three years, to give any third party free (except for a nominal charge for the cost of distribution) a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Paragraphs 1 and 2 above; or,

c) accompany it with the information you received as to where the corresponding source code may be obtained.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form alone.)

Source code for a work means the preferred form of the work for making modifications to it.For an executable file, complete source code means all the source code for all modules it contains; but, as a special exception, it need not include source code for modules which are standard libraries that accompany the operating system on which the executable file runs, or for standard header files or definitions files that accompany that operating system.

4. You may not copy, modify, sublicense, distribute or transfer the Program except as expressly provided under this General Public License. Any attempt otherwise to copy, modify, sublicense, distribute or transfer the Program is void, and will automatically terminate your rights to use the Program under this License.However, parties who have received copies, or rights to use copies, from you under this General Public License will not have their licenses terminated so long as such parties remain in full compliance.

5. By copying, distributing or modifying the Program (or any work based on the Program) you indicate your acceptance of this license to do so, and all its terms and conditions.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions.You may not impose any further restrictions on the recipients' exercise of the rights granted herein.

7. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time.Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number.If the Program specifies a version number of the license which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation.If the Program does not specify a version number of the license, you may choose any version ever published by the Free Software Foundation.

8. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this.Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

9. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW.EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES

PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU.SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

10. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to humanity, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program.It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.> Copyright (C) 19yy<name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 1, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19xx name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License.Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary.Here a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (a program to direct compilers to make passes at assemblers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989 Ty Coon, President of Vice

That's all there is to it!

FREEBSD

The compilation of software known as FreeBSD is distributed under the following terms:

Copyright (C) 1992-2005 The FreeBSD Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.IN NO EVENT SHALL AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

C-ARES

Copyright 1998 by the Massachusetts Institute of Technology.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. M.I.T. makes no representations about the suitability of this software for any purpose.It is provided "as is" without express or implied warranty.

GPLv2

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it.By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it.(Some other Free Software Foundation software is covered by the GNU Library General Public License instead.)You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price.Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have.You must make sure that they, too, receive or can get the source code.And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software.If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents.We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary.To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License.The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language.(Hereinafter, translation is included without limitation in the term "modification".)Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope.The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.(Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole.If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works.But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it.For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable.However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License.Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it.However, nothing else grants you permission to modify or distribute the Program or its derivative works.These actions are prohibited by law if you do not accept this License.Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions.You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License.If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all.For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices.Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded.In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time.Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number.If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation.If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this.Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW.EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU.SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE

WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SU CH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program.It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.> Copyright (C) 19yy<name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License.Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary.Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989 Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs.If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library.If this is what you want to do, use the GNU Library General Public License instead of this License.

ICONV

/*-
Copyright (c) 2000
* Konstantin Chuguev.All rights reserved.
*

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Konstantin Chuguev and its contributors.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
*
* iconv (Charset Conversion Library) v2.0
*/

IPFILTER

/*
Copyright (C) 1993-2001 by Darren Reed.
*
The author accepts no responsibility for the use of this software and provides it on an ``as is'' basis without express or implied warranty.
*
Redistribution and use, with or without modification, in source and binary forms, are permitted provided that this notice is preserved in its entirety and due credit is given to the original author and the contributors.
*
The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied, in part or in whole, and put under another distribution licence [including the GNU Public Licence.]
*
THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
*
I hate legalese, don't you ?
*/

LGPLv2

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA02110-1301USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL.It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it.By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it.You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price.Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights.These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you.You must make sure that they, too, receive or can get the source code.If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it.And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library.Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program.We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder.Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License.This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License.We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library.The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom.The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License.It also provides other free software developers Less of an advantage over competing non-free programs.These disadvantages are the reason we use the ordinary General Public License for many libraries.However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard.To achieve this, non-free programs must be allowed to use the library.A more frequent case is that a free library does the same job as widely used non-free libraries.In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software.For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow.Pay close attention to the difference between a "work based on the library" and a "work that uses the library".The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms.A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language.(Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it.For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope.The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it).Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is

invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application.Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole.If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works.But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library.To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License.(If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.)Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library".Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library".The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library.The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is

unrestricted, regardless of whether it is legally a derivative work.(Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License.You must supply a copy of this License.If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License.Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library.(It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library.A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it.However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system.Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities.This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute he Library except as expressly provided under this License.Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this

License.However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it.However, nothing else grants you permission to modify or distribute the Library or its derivative works.These actions are prohibited by law if you do not accept this License.Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions.You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License.If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all.For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices.Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded.In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number.If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation.If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission.For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this.Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU.SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change.You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library.It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.> Copyright (C) <year><name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA02110-1301USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary.Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990 Ty Coon, President of Vice

That's all there is to it!

LIBEVENT

Copyright 2000-2002 Niels Provos provos@citi.umich.edu All rights reserved.
*

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.
*
THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
*/

MPD

Copyright (C) 1993, Internet Initiative Japan, Inc. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the Internet Initiative Japan, Inc.The name of the IIJ may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright (c) 1995-1999 Whistle Communications, Inc. All rights reserved.

Subject to the following obligations and disclaimer of warranty, use and redistribution of this software, in source or object code forms, with or without modifications are expressly permitted by Whistle Communications; provided, however, that:(i) any and all reproductions of the source or object code must include the copyright notice above and the following disclaimer of warranties; and (ii) no rights are granted, in any manner or form, to use Whistle Communications, Inc. trademarks, including the mark "WHISTLE COMMUNICATIONS" on advertising, endorsements, or otherwise except as such appears in the above copyright notice or in the software.

THIS SOFTWARE IS BEING PROVIDED BY WHISTLE COMMUNICATIONS "AS IS", AND TO THE MAXIMUM EXTENT PERMITTED BY LAW, WHISTLE COMMUNICATIONS MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, REGARDING THIS SOFTWARE, INCLUDING WITHOUT LIMITATION, ANY AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.WHISTLE COMMUNICATIONS DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE OF, OR THE RESULTS OF THE USE OF THIS SOFTWARE IN TERMS OF ITS CORRECTNESS, ACCURACY, RELIABILITY OR OTHERWISE.IN NO EVENT SHALL WHISTLE COMMUNICATIONS BE LIABLE FOR ANY DAMAGES RESULTING FROM OR ARISING OUT OF ANY USE OF THIS SOFTWARE, INCLUDING WITHOUT LIMITATION, ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, UNITIVE, OR CONSEQUENTIAL DAMAGES, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF USE, DATA OR PROFITS, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF WHISTLE COMMUNICATIONS IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NETPERF

Copyright (C) 1993 Hewlett-Packard Company
ALL RIGHTS RESERVED.

The enclosed software and documentation includes copyrighted works of Hewlett-Packard Co. For as long as you comply with the following limitations, you are hereby authorized to (i) use, reproduce, and modify the software and documentation, and to (ii) distribute the software and documentation, including modifications, for non-commercial purposes only.

1.The enclosed software and documentation is made available at no charge in order to advance the general development of high-performance networking products.

2.You may not delete any copyright notices contained in the software or documentation. All hard copies, and copies in source code or object code form, of the software or documentation (including modifications) must contain at least one of the copyright notices.

3.The enclosed software and documentation has not been subjected to testing and quality control and is not a Hewlett-Packard Co. product. At a future time, Hewlett-Packard Co. may or may not offer a version of the software and documentation as a product.

4.THE SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS". HEWLETT-PACKARD COMPANY DOES NOT WARRANT THAT THE USE, REPRODUCTION, MODIFICATION OR DISTRIBUTION OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE A THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS. HP DOES NOT WARRANT THAT THE SOFTWARE OR DOCUMENTATION IS ERROR FREE. HP DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, WITH REGARD TO THE SOFTWARE AND THE DOCUMENTATION. HP SPECIFICALLY DISCLAIMS ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

5.HEWLETT-PACKARD COMPANY WILL NOT IN ANY EVENT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS) RELATED TO ANY USE, REPRODUCTION, MODIFICATION, OR DISTRIBUTION OF THE SOFTWARE OR DOCUMENTATION.

NTP

This file is automatically generated from html/copyright.html

Copyright Notice

jpg "Clone me," says Dolly sheepishly

Last update: 15:44 UTC Tuesday, July 15, 2003

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.
****
**
Copyright (c) David L. Mills 1992-2003*
**
Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permissionnotice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.
****

The following individuals contributed in part to the Network Time
Protocol Distribution Version 4 and are acknowledged as authors of this work.
1. [1]Mark Andrews <mark_andrews@isc.org> Leitch atomic clock controller
2. [2]Bernd Altmeier <altmeier@atlsoft.de> hopf Elektronik serial line and PCI-bus devices
3. [3]Viraj Bais <vbais@mailman1.intel.com> and [4]Clayton Kirkwood <kirkwood@striderfm.intel.com> port to WindowsNT 3.5
4. [5]Michael Barone <michael,barone@lmco.com> GPSVME fixes
5. [6]Jean-Francois Boudreault <Jean-Francois.Boudreault@viagenie.qc.ca>IPv6 support
6. [7]Karl Berry <karl@owl.HQ.ileaf.com> syslog to file option
7. [8]Greg Brackley <greg.brackley@bigfoot.com> Major rework of WINNT
port. Clean up recvbuf and iosignal code into separate modules.
8. [9]Marc Brett <Marc.Brett@westgeo.com> Magnavox GPS clock driver
9. [10]Piete Brooks <Piete.Brooks@cl.cam.ac.uk> MSF clock driver, Trimble PARSE support
10. [11]Reg Clemens <reg@dwf.com> Oncore driver (Current maintainer)
11. [12]Steve Clift <clift@ml.csiro.au> OMEGA clock driver
12. [13]Casey Crellin <casey@csc.co.za> vxWorks (Tornado) port and help with target configuration
13. [14]Sven Dietrich <sven_dietrich@trimble.com> Palisade reference clock driver, NT adj. residuals, integrated Greg's Winnt port.
14. [15]John A. Dundas III <dundas@salt.jpl.nasa.gov> Apple A/UX port
15. [16]Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de> Linux port
16. [17]Dennis Ferguson <dennis@mrbill.canet.ca> foundation code for NTP Version 2 as specified in RFC-1119
17. [18]John Hay <jhay@@icomtek.csir.co.za> IPv6 support and testing
18. [19]Glenn Hollinger <glenn@herald.usask.ca> GOES clock driver
19. [20]Mike Iglesias <iglesias@uci.edu> DEC Alpha port
20. [21]Jim Jagielski <jim@jagubox.gsfc.nasa.gov> A/UX port
21. [22]Jeff Johnson <jbj@chatham.usdesign.com> massive prototyping overhaul
22. [23]Hans Lambermont <Hans.Lambermont@nl.origin-it.com> or
[24]<H.Lambermont@chello.nl> ntpsweep
23. [25]Poul-Henning Kamp <phk@FreeBSD.ORG> Oncore driver (Original author)
24. [26]Frank Kardel [27]<Frank.Kardel@informatik.uni-erlangen.de> PARSE <GENERIC> driver (14 reference clocks), STREAMS modules for PARSE, support scripts, syslog cleanup
25. [28]William L. Jones <jones@hermes.chpc.utexas.edu> RS/6000 AIX modifications, HPUX modifications
26. [29]Dave Katz <dkatz@cisco.com> RS/6000 AIX port
27. [30]Craig Leres <leres@ee.lbl.gov> 4.4BSD port, ppsclock, Magnavox GPS clock driver
28. [31]George Lindholm <lindholm@ucs.ubc.ca> SunOS 5.1 port
29. [32]Louis A. Mamakos <louie@ni.umd.edu> MD5-based authentication
30. [33]Lars H. Mathiesen <thorinn@diku.dk> adaptation of foundation code for Version 3 as specified in RFC-1305
31. [34]Danny Mayer <mayer@ntp.org>Network I/O, Windows Port, Code Maintenance
32. [35]David L. Mills <mills@udel.edu> Version 4 foundation: clock discipline, authentication, precision kernel; clock drivers: Spectracom, Austron, Arbiter, Heath, ATOM, ACTS, KSI/Odetics; audio clock drivers: CHU, WWV/H, IRIG
33. [36]Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de> VMS port
34. [37]Jeffrey Mogul <mogul@pa.dec.com> ntptrace utility
35. [38]Tom Moore <tmoore@fievel.daytonoh.ncr.com> i386 svr4 port
36. [39]Kamal A Mostafa <kamal@whence.com> SCO OpenServer port
37. [40]Derek Mulcahy <derek@toybox.demon.co.uk> and [41]Damon Hart-Davis <d@hd.org> ARCRON MSF clock driver
38. [42]Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de> monitoring/trap scripts, statistics file handling
39. [43]Dirce Richards <dirce@zk3.dec.com> Digital UNIX V4.0 port
40. [44]Wilfredo Sánchez <wsanchez@apple.com> added support for NetInfo
41. [45]Nick Sayer <mrapple@quack.kfu.com> SunOS streams modules
42. [46]Jack Sasportas <jack@innovativeinternet.com> Saved a Lot of space on the stuff in the html/pic/ subdirectory
43. [47]Ray Schnitzler <schnitz@unipress.com> Unixware1 port
44. [48]Michael Shields <shields@tembel.org> USNO clock driver
45. [49]Jeff Steinman <jss@pebbles.jpl.nasa.gov> Datum PTS clock driver
46. [50]Harlan Stenn <harlan@pfcs.com> GNU automake/autoconfigure makeover, various other bits (see the ChangeLog)
47. [51]Kenneth Stone <ken@sdd.hp.com> HP-UX port
48. [52]Ajit Thyagarajan <ajit@ee.udel.edu>IP multicast/anycast support

49. [53]Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp>TRAK clock driver
50. [54]Paul A Vixie <vixie@vix.com> TrueTime GPS driver, generic TrueTime clock driver
51. [55]Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de> corrected and validated HTML documents according to the HTML DTD

References

1. mailto:%20mark_andrews@isc.org
2. mailto:%20altmeier@atlsoft.de
3. mailto:%20vbais@mailman1.intel.co
4. mailto:%20kirkwood@striderfm.intel.com
5. mailto:%20michael.barone@lmco.com
6. mailto:%20Jean-Francois.Boudreault@viagenie.qc.ca
7. mailto:%20karl@owl.HQ.ileaf.com
8. mailto:%20greg.brackley@bigfoot.com
9. mailto:%20Marc.Brett@westgeo.com
10. mailto:%20Piete.Brooks@cl.cam.ac.uk
11. mailto:%20reg@dwf.com
12. mailto:%20clift@ml.csiro.au
13. mailto:casey@csc.co.za
14. mailto:%20Sven_Dietrich@trimble.COM
15. mailto:%20dundas@salt.jpl.nasa.gov
16. mailto:%20duwe@immd4.informatik.uni-erlangen.de
17. mailto:%20dennis@mrbill.canet.ca
18. mailto:%20jhay@icomtek.csir.co.za
19. mailto:%20glenn@herald.usask.ca
20. mailto:%20iglesias@uci.edu
21. mailto:%20jagubox.gsfc.nasa.gov
22. mailto:%20jbj@chatham.usdesign.com
23. mailto:Hans.Lambermont@nl.origin-it.com
24. mailto:H.Lambermont@chello.nl
25. mailto:%20phk@FreeBSD.ORG
26. http://www4.informatik.uni-erlangen.de/%7ekardel
27. mailto:%20Frank.Kardel@informatik.uni-erlangen.de
28. mailto:%20jones@hermes.chpc.utexas.edu
29. mailto:%20dkatz@cisco.com
30. mailto:%20leres@ee.lbl.gov
31. mailto:%20lindholm@ucs.ubc.ca
32. mailto:%20louie@ni.umd.edu
33. mailto:%20thorinn@diku.dk
34. mailto:%20mayer@ntp.org
35. mailto:%20mills@udel.edu
36. mailto:%20moeller@gwdgv1.dnet.gwdg.de
37. mailto:%20mogul@pa.dec.com
38. mailto:%20tmoore@fievel.daytonoh.ncr.com
39. mailto:%20kamal@whence.com
40. mailto:%20derek@toybox.demon.co.uk
41. mailto:%20d@hd.org
42. mailto:%20Rainer.Pruy@informatik.uni-erlangen.de
43. mailto:%20dirce@zk3.dec.com
44. mailto:%20wsanchez@apple.com
45. mailto:%20mrapple@quack.kfu.com
46. mailto:%20jack@innovativeinternet.com
47. mailto:%20schnitz@unipress.com
48. mailto:%20shields@tembel.org
49. mailto:%20pebbles.jpl.nasa.gov
50. mailto:%20harlan@pfcs.com
51. mailto:%20ken@sdd.hp.com
52. mailto:%20ajit@ee.udel.edu
53. mailto:%20tsuruoka@nc.fukuoka-u.ac.jp
54. mailto:%20vixie@vix.com
55. mailto:%20Ulrich.Windl@rz.uni-regensburg.de

© Copyright NETASQ 2006